PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Department of Computer Science
Proceedings of 2nd International Conference on Recent Innovations in Computer Science &Technology (ICRICT 2024)
29th to 31st January
2024ISBN: 978-81-
968265-0-5
URL: https:/ pbsiddhartha.ac.in/ICRICT24/

INDEX, VOLUME II

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Intelligent Toll Collection System for Moving Vehicles in India

I.JITENDRA NAIDU
23DSC02, M.Sc. (Computational Data Science)
Department of Computer Science
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India
jitendranaidu9774@gmail.com

KOGNTI GAYATHRI
Programmer
Department of Computer Science
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India
kgayathri@pbsiddhatha.ac.in

P. BHARGAVI
23DSC05, M.Sc. (Computational Data Science)
Department of Computer Science P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India
Bhargavibharu741@gmail.com

ABSTRACT: This Paper Proposes an Automatic Toll Collection System to Debit the Toll of Moving Vehicles at A Toll Plaza in India. An Effective Approach Is Presented Here to Localize the License Plate of Vehicles. A Database Has Been Created and Linked to Test the Performance of The Prototype Toll Collection System of Moving Vehicles. The Database Includes the Number of Vehicles, Vehicle Owner's Name, The Unique Identification Number of The Vehicle Owners, Their Mobile Number and Balance of The Linked Bank Account. The Results Show A Significant Reduction in The Vehicle Waiting Time, Queue Length, Fuel Wastage, And Excretion of Pollution at A Toll Plaza. In Future the System Can Be Used for The Theft Control. The Challenges Faced by Vehicle Challans and Brings A Better and Automated Solution for Vehicle Challans. A Simple Tweak in The Fastag system, Can Bring A Vast Change to Entire Transport System. In Order to Apply This System A Modification in Existing TOLL System Has to Be Achieved Using Additional Equipment (Machine Learning Capable System and Secure Database).

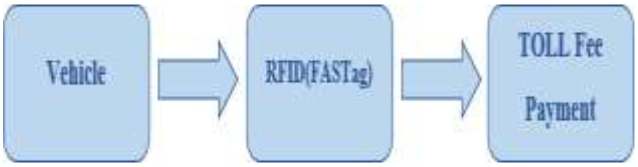
KEYWORDS: ALPR, Intelligent toll collection system, LabVIEW, Vision assistant, Morphological filters, Vision acquisition, MyRio, FASTag, Object detection, YOLO, TOLL, Object detection, CNNs.

I. INTRODUCTION

For Indian drivers, excessive traffic is a regular occurrence, thus having to wait in long lines at toll booths is always a hassle and a waste of time. The government has implemented FASTag, an RFID-powered tag, to address this issue and make the toll the experience of the plaza is less complicated. You have to drive through the toll booth, attach the tag to your windscreen, and you're done! The plaza's scanner will recognize the tag, which will automatically deduct the toll fee from your bank account. Having said that, the system is still quite young and therefore susceptible to some mistakes and failures. The card might be easily lost, damaged, or stolen because it is attached to your windscreen. Due to manual toll collection system and their slow processing, the heavy traffic jams and long queue at the toll plazas has become a great challenge in India. This is also a cause of long waiting time and wastage of fuels during toll collect.

Apart from it, this is also increasing the excretion of pollution and decrease the speed of the highways which may be the inadequate quality of the food products specially milk products. Many countries like Japan, Korea, and America etc. are doing research in this field. The paper presents an automatic toll collection system (ATCS) can play a vital role by reducing the toll processing time of the moving vehicle at toll plaza. The automatic license plate recognition (ALPR) approach is based on the reading of the number plate of a moving car using various image processing techniques. There is unique identity card (i.e., Aadhaar Card) for Indian citizen. As per the policy of Indian government, every Indian must link their mobile number, bank account and vehicles with his/her Aadhaar Card. This paper proposed an approach to identify the owner of the vehicle, his bank account which is registered license plate of the vehicle and linked Aadhar card and automatically deduction of the toll amount from his bank account which is liked with the Aadhar card. It means every vehicle in India is directly or indirectly linked with bank account of the vehicle owner. Many countries have applied different methods for toll collections like travel time estimation and prediction (TTEP) and Global System for Mobile Communications (GSM) based car tracking, automatic vehicle identification, light mirror technique etc. but here is the most famous approach is electronic toll collection (ETC). Norway has been the world's pioneer in the widespread implementation of this technology. First ETC was introduced in Bergen, in 1986. For Taiwan, a comparison study of electronic toll collection (ETC) and manual toll collection (MTC) was conducted. Some of the benefits of these techniques have been addressed here. There are

numerous benefits to the use of license plate recognition software, but there are also some disadvantages. The time-consuming task of manually recording license plate numbers can be eliminated with automatic license plate recognition. The actual registration number is virtually hard to see, especially when a car is rushing past. Automatic number plate recognition systems capture the numbers of vehicles in real time as well as offer a detailed picture of traffic patterns. There is still and video footage in many automatic license plate recognition systems. Some are designed to take photographs when a vehicle accelerates runs a red light, or makes an incorrect turn. The recording is steady in a variety of camera positions and angles, as well as in a variety of weather situations. Traffic departments and legal counsel can both benefit from video footage. Serial traffic violators are determined by license plate recognition. The system also aids with reactive security. Inspections, forensics, investigations, and legal proceedings are all examples of this. Automatic license plate recognition appears to be a need no matter how you look at it. With these some drawbacks are also.



II. FASTAG

Rapid and exciting changes are being made to the Indian economy's face. As a result of the digital transition, our lives are now more convenient and effective, and routine tasks are no longer taxing. Attempt to recall the last time you had to endure hours-long lines. Or when you needed to visit several different stores to acquire a small number of items? As a result, daily tasks are now simple, quick, and convenient thanks to widespread digitization across many industries. And now it is being applied on the highways, away from your house. Around 615 toll plazas on national highways across the nation have installed the FASTag technology adjustments. The administration is anxious to adopt a cashless system. The steps performed in ATCS are automatic vehicles identification and their classification, transaction processing and violation enforcement. The automatic license plate recognition approach is used for the first step. The LABVIEW is used with the vision assistant and vision acquisition modules and my re-configurable Input/Output (MyRIO) is used as the hardware module. Morphological filters such applied to make the captured image smooth and optical character reader (OCR) is used to read the license plate of the vehicle in real time. A database has been created using Microsoft SQL Server Management Studio and linked to the program using Open Database Connectivity (ODBC) drivers to test the performance of the prototype toll collection system of moving vehicles. LABVIEW in this system is providing the user-friendly environment. The fast response and efficient detection are the additional benefits of this system.

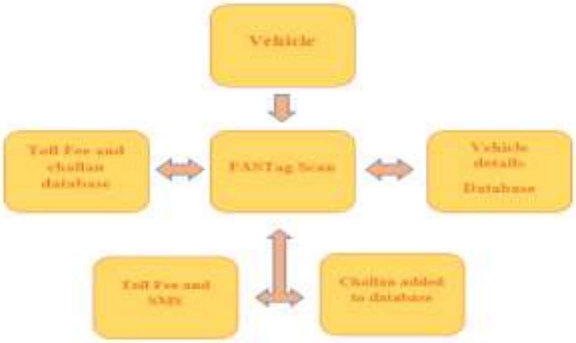
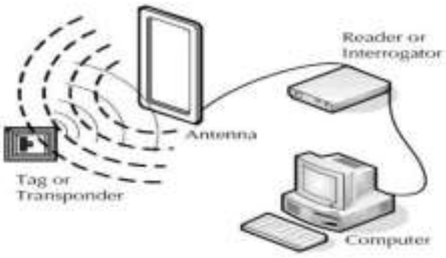
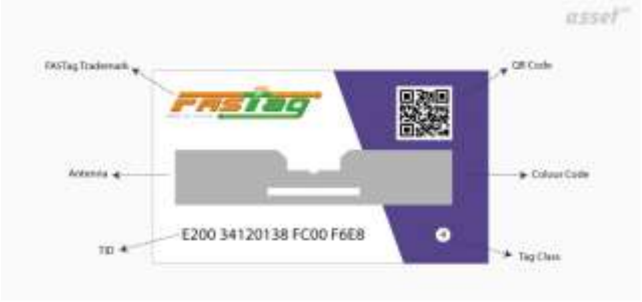


Image 1: Basic TOLL concept system
Image 2: Advance TOLL &Challan system concept

III. WORKING

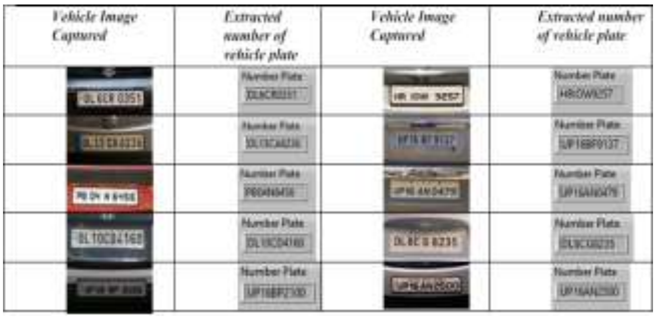
RFID technology enables a device to capture the digital data encoded in RFID tags using the radio waves. RFID is catalogued under a wide-ranging technology called Automatic Identification and Data Capture (AIDC). It uses radio waves to automatically detect tags, collect data about them and enter the collected data straightforwardly into the computer systems with the help of a micro controller or processorFASTag is fixed to the windscreen of the vehicle and is associated to a prepaid account. Toll payments are made over RFID, as the vehicle passes through the toll gate, which means you do not have to stopover at a toll plaza on your journey. The prepaid FASTag account will be deducted for the transaction which makes payments simpler. As far as four-wheelers are concerned FASTag will work fine then what about two-wheeler and vehicles that doesn't have RFID baked into vehicle. For situations like that I came up with a solution, which involves in image processing and machine learning.





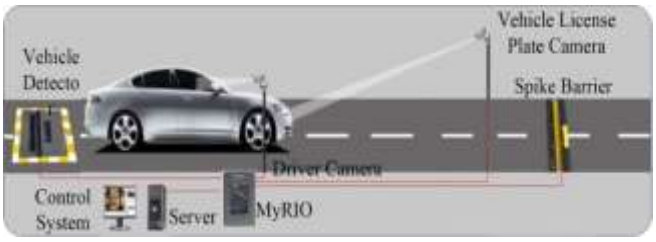
IV. AUTOMATIC LICENSE PLATE RECOGNITION

The ALPR approach has three steps: The image acquisition of moving vehicle, extraction of license plate and the recognition of the license plate. The image acquisition is the first step and can be done in many ways such as an image acquisition card can be used to convert video signals into digital images, or a sensing system can be developed using two charge coupled devices (CCDs) and a prism. The sensing systems can take images in wide range of illuminations and without blurring.


Vehicle Image Captured
Extracted number of vehicle plate
Vehicle Image Captured
Extracted number of vehicle plate
Number Plate

a. Separation of the pixels has been done into two clusters based on the threshold.
b. Finding the means of the clusters
c. Finding difference of square of the means
d. Multiply by the number of pixels in one cluster to the other.

The license plate extraction is the most important task of the ALPR approach. It is difficult in India as compared to other countries due to lack of size and color specification of vehicles number plant because many colors are allowed for the same. The vehicle number plate can be extracted by using many features such as scale-shape analysis. Here in-built laboratory virtual instrument engineering workbench (LabVIEW) tool is used to convert the captured image into gray scale as well as to the binary. A morphological filter such as remove small objects, particle filtering is used to smooth the captured image of the vehicle plate. The shape analysis can eliminate the need for fix specification of number plate to much extent. Further edge detection is also used in some papers, but it leads to more errors. Two neural network filters can also be used with an after processer to combine the filtered images to extract number plates, but it needs horizontal to vertical ratio of plate size. The shape detection is an inbuilt tool provided in the Lab VIEW to identify the various shapes in the image with variable size.



The rectangle is searched for finding the number plate in the captured image. Moreover, various parameters are given as input like ranges for width and height of rectangle, window size and step sizes for row and column. The selection of the step size is based on the number of pixels in the moving window during each of the iteration to find out the rectangle. There are three filters are used to recognize the number plate of moving vehicle. The remove small particles (RSP) filter is the low pass filter which removes small the particles according to their widths compared to the specified by a parameter called filter size. For a given filter size N, the filter removes all particles with size less than or equal to (N-1) in (N-1)/2 erosions. Moreover, the particle filtering is used to filter the particles from the captured image. The particles can be filtered by setting the ranges for center of mass, width of particle, height of particle, perimeter, or area of the particle. The particles falling in the ranges are removed and the rest remain with the same values. The equalization is the third step of the number plate reorganization system. The equalize function changes the gray-level values of the pixels to make them evenly distributed in the defined range i.e., 0 to 255 for an 8-bit image. It is used to improve the contrast in the image. License Plate recognition can be done by many methods like Statistical pattern recognition template matching, neural network recognition and optical character reader (OCR). The most simple and effective way of doing character recognition is OCR. It is the mechanical or electrical conversion of the handwritten, typed or printed text into the machine-encoded text. LabVIEW’s inbuilt OCR tool is used in this paper. The tool has many benefits like options for selecting the threshold for the characters to be recognized and can set the ranges of width and height of the characters to be read. There are two segmenting theorems given-shortest segment for reading close characters and Legacy auto split for reading tilted characters. The ALPR approach is mostly performed in MATLAB, but LabVIEW is better option because it provides virtual platform and easy way to interface with the hardware for image processing applications.

V. SYSTEM CONFIGURATION

The prototype of the automatic toll collection system consists of a vehicle detector, camera, MyRIO, computer and vehicle barrier system. The vehicle detector is mounted at a desired distance from the barrier. It generates a signal as the vehicle reached at the desired location and sends the signal to the MyRIO to activate the camera. Once the camera is activated, it adjusts the brightness and then capture the picture of the moving vehicle. Here a simple camera (laptop web cam) is to capture the picture, but high-speed cameras which can capture better quality picture at the interval of 1ms. The captured image of the vehicle is transferred to the MyRIO. This executes the program for the extraction of number plate from the captured image. Further, it also does a real time processing on the captured image to extract the ‘text’ from the license plate. It is a realtime embedded evaluation board made by National Instruments.

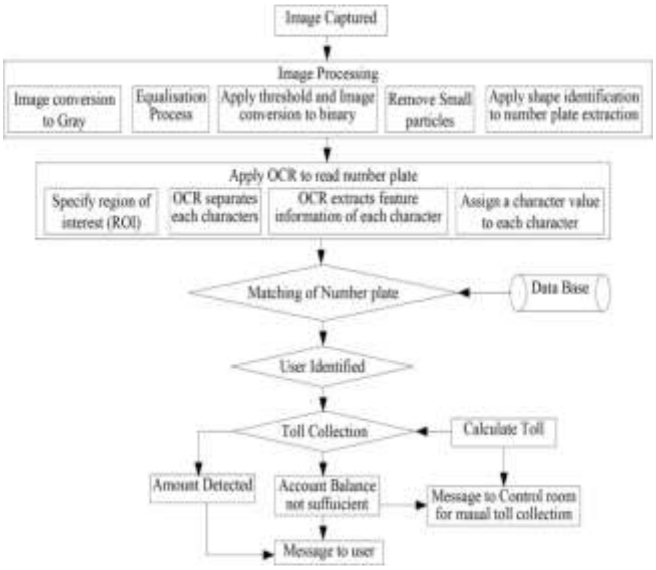
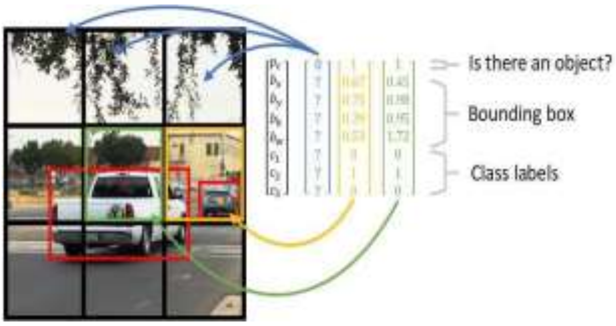


Image Captured
Image Processing
Image conversion to Gray
Equalisation Process
Apply threshold and Image conversion to binary
Remove Small particles
Apply shape identification to number plate extraction
Apply OCR to read number plate
Specify region of interest (ROI)
OCR separates each characters
OCR extracts feature information of each character
Assign a character value to each character
Matching of Number plate
Data Base
User Identified
Toll Collection
Calculate Toll
Amount Detected
Account Balance not sufficient
Message to Control room for maual toll collection
Message to user

VI. OBJECT DETECTION

For vehicles that don't have any FASTag will be scanned using object detection. In order to so 'yolo object detection algorithm' is used where we will train a set of images [5]. In order to do this, we need machine(computer) capable of doing machine learning tasks. First, we can train images and get the trained weight file. With help of weights files, we can proceed with the object detection.

1.is there an object?
2.boundind box
3.classlables



VII. Mathematical model for threshold equalisation

Let {X} be a discrete grayscale image and let the number of occurrences of gray level l be Nl. The probability of an occurrence of a pixel of
level l in the image can be expresses as
Pi(l) = P(i = l) = Nl
N; 0 ≤ l < L (1)
L is the total number of gray levels (256 for an 8-bit image), N being the total number of pixels in the image and
Pi(l) being in fact the image's histogram for pixel value l, normalized to [0,1]. The cumulative distribution function (CDF) corresponding to Pl can be defined as:
cdfi(l) = ∑i
k=0Pi(k) (2)
The new image {j} with a flat histogram can be produced by creating a transformation of the form j = H(i). Such an image would have a linearized cumulative distribution function (CDF) across the value range, i.e.
cdfj(l) = lα (3) for some constant α.
The properties of the CDF allow us to perform such a transform; it is defined as:
cdfj(j
′
) = cdfj(H(m)) = cdfi(m) (4)
where m is in the range [0, L]. Notice that T maps the levels into the
range [0, 1], since we used a normalized histogram of {i}. To map the
values back into their original range, the following simple transformation needs to be applied to the result:
j
′
= j(max{X} − min{X}) + min{X} (5)
Now, threshold is applied to the image to convert it into binary form.
For this purpose, Otsu's global thresholding method is used. The value of the threshold is taken in such a way that the whole of the number plate gets covered. The Otsu's method sets the threshold so that each cluster is too tight, to minimizing their overlap. This is not changing the distributions but tries to adjust where to separate them (the threshold). The goal is to select the threshold to minimize the combined spread.
The within variance can be calculated as: σ2
within(T) = nB(T)σ2
B(T) + nO(T)σ2
O(T) (6)
where, nB (T) is the total number of background pixel in the image and can be calculated as:
nB(T) = ∑T− 1
i=0 p(i) (7)
While, no (T) is the total number of foreground pixel in the image and can be calculated as:
nO(T) = ∑N− 1
i=T p(i) (8)
The σ2
B(T) is the variance of the pixels in the background (below Threshold) in the image.
The σ2O(T) is the variance of the pixels in the
foreground (above Threshold) in the image and [0, N-1] is the range of intensity level.
To get the between-class variance (σ2
Between(T)), the within-class
variance (σ2
within(T)), has been subtracted from the total variance
(σ2(T)), of the combined distribution in the image.
σ2

Between(T) = σ2 − σ2
within(T) (9)
σ2
Between(T) = nB(T)|μB(T) − μ|
2 − nO(T)[μO(T) − μ]
2 (10)
where, μ is the mean of the variance. The between-class variance
(σ2
Between(T)), is simply the weighted variance of the cluster means
themselves around the overall mean and can be calculated as:
μ = nB(T)μB(T) + nO(T)μO(T) (11)
The between-class variance can be obtained after solving equation
(10) and (11) and can be expressed as:
σ2
Between(T) = nB(T)nO(T)[μB(T) − μO(T)]2 (12)
The selection of the potential threshold (T) has been done using the following steps:

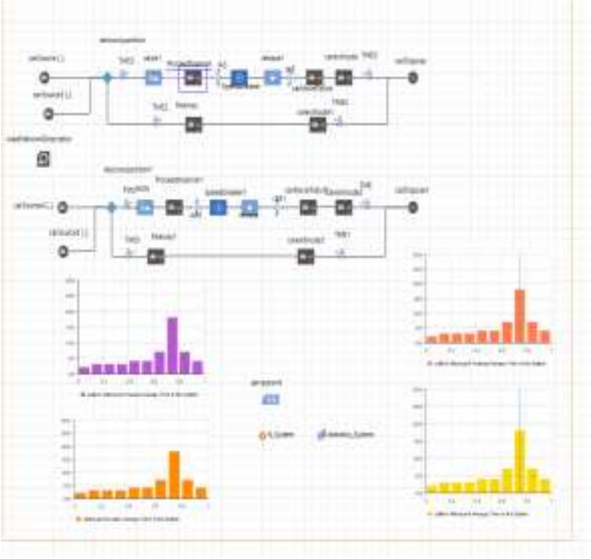
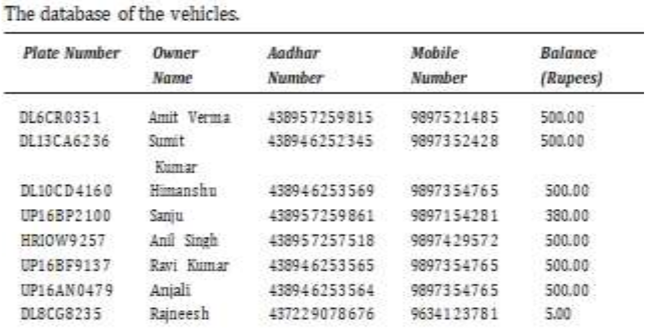


Fig: Process and Statistics

VIII. ANALYSIS OF AUTOMATIC LICENSE PLATE RECOGNITION SYSTEM

The performance of the automatic license plate recognition (ALPR) system has been tested with 10 vehicles of 4 different states such as the Uttar Pradesh (4 vehicles), Delhi (04 vehicles), Punjab (01 vehicle) and Haryana (01 vehicle) of India as mentioned table. The captured images are picked of different vehicles with different kinds of license plates and in different conditions. For example, the vehicles of license plate DL6CR0351, DL13CA6236, DL10CD4160, consists of their licensed number and other text "IND" while the vehicles of license plate UP16AN2500 consist of their licensed number and other text "IND" as well as text "उत्तरप्रदेशसरकार". The remaining vehicles of license plate PB04N6456, UP16BP2100, HRIOW9257, UP16BF9137, UP16AN0479 and DL8CG8235. Apart from it, the text size, text, style and unequal space between two characters. But the ALPR system correctly identified the license number of all the vehicles after elimination of the remaining text as mentioned in Table is the function of system length, length of queue, waiting.



The database of the vehicles.

Plate Number	*Owner Name*	*Aadhar Number*	*Mobile Number*	*Balance (Rupees)*
DL6CR0351	Amit Verma	438957259815	9897521485	500.00
DL13CA6236	Sumit Kumar	438946252345	9897352428	500.00
DL10CD4160	Himanshu	438946253569	9897354765	500.00
UP16BP2100	Sanju	438957259861	9897154281	380.00
HRIOW9257	Anil Singh	438957257518	9897429572	500.00
UP16BF9137	Ravi Kumar	438946253565	9897354765	500.00
UP16AN0479	Anjali	438946253564	9897354765	500.00
DL8CG8235	Rajneesh	437229078676	9634123781	5.00

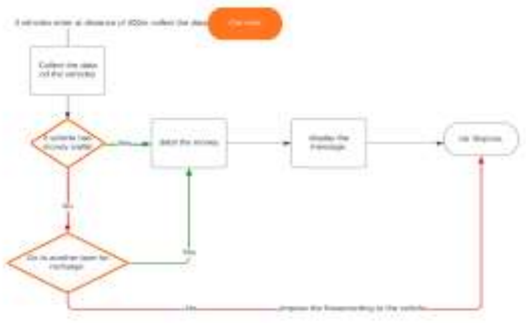


Fig: Flow chart

IX. DISCUSSIONS

The detail description of fuel consumption and pollution generation for various vehicle arrival rates for a toll plaza system rated with 65 vehicles/hour can be found in table. The fuel consumption and production of the pollution is the function of system length, length of queue, waiting time increases with respect to the vehicle arrival rate at the toll plaza. The simulation result shows that the automatic toll collection system saves the fuel approximately 22.35 liter per day with the vehicle arrival rate of 40 vehicles/hour. While the fuel consumption at the toll plaza decreased 15.6, 20.97 and 31.4 times with ATCS as compared to MTCS for the vehicle arrivals rate of 45, 50, 55 vehicles/hour respectively. The pollution production at the toll plaza during toll collection reduced 11-31 times with the ATCS as compared to the MTCS as mentioned in table. Approximately 133 kg per day less pollution generates at toll plaza with ATCS as compared with MTCS for the vehicle arrival rate 55 vehicles/hours. In case of with the 60 vehicles/hour arrival rate, the CO2 emission reduced 251.4 Kg/Day at the toll plaza with ACTS. The human body excretes 0.92 Kg/day. It means a reduction in CO2 by the ATCS at the toll plaza of one lane is equal the CO2 excrete by 273 humans per day. In other words, it decreases the CO2 of 273 humans on the ground. In general, every toll plaza has 8-10 lanes, therefore, the maximum total CO2 at a toll plaza with ATCS will decrease 2514 Kg/Day (i.e., 2730 humans per day). As shown in table and table the time consumption and fuel consumption at toll plaza decreases it increases average movement of the speed of the vehicles and again decrease the fuel consumption.

X. CONCLUSION

This paper proposes an automatic toll collection system (ATCS) for toll plaza to collect the tolls of moving vehicles. The optical character reader (OCR) with small particle filter shows better performances in higher accuracy and small average inspection time (fast speed) for number plate extraction of a moving vehicle. The ATCS decreased, the system length, length of queue, vehicle waiting time at the toll plaza in comparison to manual toll collection system (MTCS). As the fuel consumption and excretion of the pollution at the toll plaza depends on the waiting time of the vehicles. Therefore, ATCS further decrease the wastage of fuel and excretion of pollution at the toll plaza. There are many challenges to be addressed for implementation of the automatic toll collection system such as linking of the vehicle license with the bank account of the user. Apart from it, the proposed system requires high resolution cameras. The ATCS can also be applied in parking areas and for security purposes in buildings and government offices by doing some minor changes. when compared to RFID based FASTag, DSRC based FASTag results in avoidance of congestion at toll gates. The waiting time of vehicles at toll boots is less when DSRC based FASTag is used. From the graphs, average speed of the vehicles, average time of the vehicles, mean of the vehicles, median of the vehicles is obtained. From average time of the vehicles, there by concluding that DSRC technology will be more useful in tollgate congestion rather than RFID tollgate system. By installing additional tolls or checkpoints, DSRC systems can be readily extended to other routes or across neighboring regions. As a result of the potentially large number of toll sites required to offer adequate coverage, expanding these kinds of systems to cover far greater areas is less cost effective.

XI. REFERENCES

[1] A. Arya, N. Jaggi and I. Srikanth, "EMI shielding for DSRC Electronic Toll Collection using grid-based Carbon fibre/epoxy composites," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2018.

[2] M. E. Harikumar, M. Reguram and P. Nayar, "Low-cost traffic control system for emergency vehicles using ZigBee," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018.

[3] Guo-Huang Hsu, Liang-Rui Lin, Rong-Hong Jan and Chien Chen, "Design of ETC violation enforcement system for non-payment vehicle searching," 2013 15th International Conference on Advanced Communications Technology (ICACT), 2013.

[4] V. Astarita, M. Florian and G. Musolino, "A microscopic traffic simulation model for the evaluation of toll station systems," ITSC 2001.2001 IEEE Intelligent Transportation Systems. Proceedings (Cat. No.01TH8585), 2001.

[5] E. R., Earn, P. K., & Kim, H. J. (1994). "Automatic recognition of a car license plate using color image processing".In , 2. IEEE International Conference on Image Processing 1994.

[6] Chauhan, K., &Chauhan, R. K. (2020). “Design and Development of Two Levels Electronic Security and Safety System for Buildings”. International Journal of Electronic Security and Digital Forensics, Inderscience,

[7] L. R. Lin, G. H. Hsu, R. H. Jan and C. Chen, "A novel non-payment vehicle searching method for multilane-free-flow electronic-toll-collection systems," 2012 14th International Conference on Advanced Communication Technology (ICACT), 2012.

[8] D. Dismantoro, I. Pratomo and S. Sumpeno, "Minimizing Toll Payment Queue using GPS-Based Mobile Applications," 2020 Fifth International Conference on Informatics and Computing (ICIC), 2020.

IoT-Based Health Monitoring System

SRAVANI MAREDDY
23MCA16,Student,MCA
Dept. of Computer Science
P.B.Siddaratha college of arts & science
Vijayawada,A.P,India
Sravanimareddy1918@gmail.com

KOTHAPALLI ROHITHA
23MCA13, Student, M.C.A
Dept. of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
rohithakothapalli1@gmail.com

MALLA BHARAGAVI
23MCA15,Student, M.C.A
Dept. of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
bharagavimalla03@gmail.com

ABSTRACT: In Recent Years, Heightened Awareness of Escalating Health Concerns Has Prompted A Greater Focus on Personal Well-Being. This Paper Details the Conception and Execution of an Iot-Driven Health Monitoring System Integrating Temperature and Pulse Rate Sensors. Continuous Monitoring of the Patient's Vital Signs Enables Real-Time Updates for the Doctor, Accessible Remotely. In Case of Abnormal Health Conditions, Instant Alerts are Dispatched Via Email, Allowing the Doctor to Promptly Diagnose Issues and Potentially Save Lives. This Project Aims to Facilitate Timely Communication of The Patient's Health Status to The Doctor, Enabling Swift Intervention in Case of Anomalies.

KEYWORDS: Health monitoring, IoT, Temperature sensor, Pulse rate sensor, Remote monitoring, Real-time updates, Abnormality alerts, E-mail notifications, Timely communication, Patient's condition, Doctor intervention.

I. INTRODUCTION

With the escalating concerns about health and the increasing prevalence of diseases, the need for continuous health monitoring has become paramount. This paper introduces an IoT-based Health Monitoring System designed to address this imperative. In response to the challenge that doctors face in monitoring patients continuously, especially those requiring constant attention, the proposed system integrates temperature and pulse rate sensors. These days, the expansion of innovations by wellbeing specialists is exploiting these electronic devices [1].The paper details a health monitoring system leveraging IoT, incorporating wearable sensors for measuring EMG, ECG, temperature, blood glucose levels, and muscle activity. Cloudlet computing and processing, alongside pattern recognition and machine learning algorithms, were employed for data storage and analysis [2]. The significance of this IoT-based health monitoring system lies in its ability to bridge the gap between constant patient surveillance and the demands on a doctor's time. By providing timely updates and alerts, the system not only enhances patient care but also contributes to optimizing doctors' responsiveness and, consequently, improving overall healthcare outcomes. While individuals with coronavirus illness feel ill, their oxygen levels are often insufficient [3]. This paper offers insights into healthcare management technology, aiming to safeguard patients against potential health issues and assist physicians in administering suitable doses at the right times throughout a patient's life [4].

1.1 HEARTBEAT SENSOR

A heartbeat sensor is employed to measure the digital output of heart beats per minute. It includes two LEDs emitting red and IR light. The calculation of the heartbeat rate relies on the variation in IR light caused by the contraction and relaxation of the heart, determining the pulse rate based on the increase or decrease in oxygenated blood.

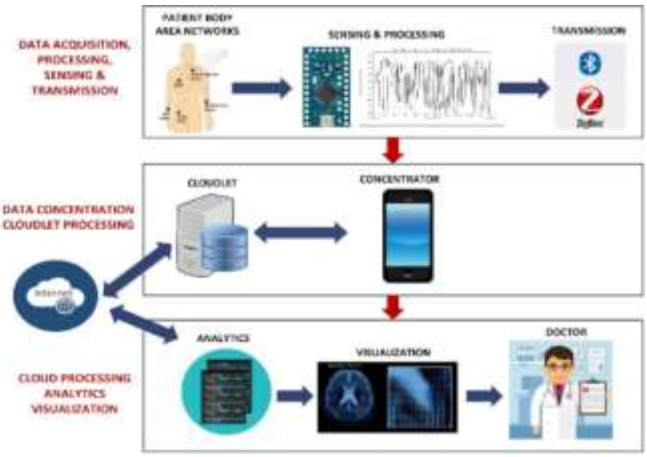

DATA ACQUISITION, PROCESSING, SENSING & TRANSMISSION
PATIENT BODY AREA NETWORKS
SENSING & PROCESSING
TRANSMISSION
ZigBee
DATA CONCENTRATION CLOUDLET PROCESSING
CLOUDLET
CONCENTRATOR
Internet
CLOUD PROCESSING ANALYTICS VISUALIZATION
ANALYTICS
VISUALIZATION
DOCTOR

Fig. 1. Wearable Health Monitoring System with IoT Integration and Messaging Functionality.

1.2 Data acquisition, processing, sensing & transmission:

The data lifecycle involves some key stages:

Acquisition, processing, sensing, and transmission. Sensors gather real-world data, which is then acquired and processed locally or on edge devices. Following processing, the information is sensed to extract meaningful insights. Finally, the processed data is transmitted to central systems or the cloud for further analysis, storage, and decision-making in the broader IoT ecosystem. This cyclic process forms the foundation for efficient and responsive IoT applications.

1.3 Data concentration cloudlet processing:

A heartbeat sensor is employed to measure the digital output of heart beats per minute. It includes two LEDs emitting red and IR light. The calculation of the heartbeat rate relies on the variation in IR light caused by the contraction and relaxation of the heart, determining the pulse rate based on the increase or decrease in oxygenated blood.

1.4 Cloud processing analytics visualization:

In IoT, Cloud processing encompasses analytics and visualization to derive meaningful insights from data. The data collected from IoT devices is processed in the cloud, leveraging analytical tools to extract valuable information. Subsequently, visualization techniques are applied to represent these insights in a comprehensible manner, aiding decision-making. This integrated approach in cloud computing enhances the efficiency and effectiveness of IoT applications by providing a centralized platform for advanced processing, analytics, and intuitive data representation.

1.5 Role of IoT in Health Monitoring:

IoT plays a crucial role in health monitoring, functioning as a monitoring and assessment tool to track the real-time condition of structures, machinery, or equipment. It gathers, analyzes, and transmits diverse data parameters related to the service condition, leading to cost optimization in repair and maintenance. This technology minimizes the need for manual intervention, enhances efficiency, and extends the lifespan of machinery by promptly identifying and addressing issues.[5]

II. TYPES OF VISIONS FOR IOT BASED HEALTH MONITORING SYSTEM:

Visions in the context of IoT-based Health Monitoring Systems can be categorized into:

2.1 Remote Patient Surveillance:

Enabling healthcare professionals to monitor patients remotely, enhancing accessibility and reducing the need for frequent hospital visits. I-Body, the focus is on continuous monitoring to swiftly identify early signs of health issues, empowering individuals and healthcare providers to take proactive measures for better health outcomes.

2.2 Predictive Analytics:

Applying machine learning to historical health data predicts potential health issues, allowing for preventive measures and timely interventions. Leveraging I-Body data for predictive analysis involves using machine learning to foresee potential health issues. This capability enables timely preventive measures and interventions based on individual health trends.

2.3 Efficient Healthcare Delivery:

Streamlining healthcare processes through IoT can lead to more efficient and cost-effective delivery of medical services, improving overall healthcare systems.

2.4 Data-Driven Research:

Aggregated data from large-scale IoT health systems can contribute to medical research, fostering a better understanding of diseases and treatment effectiveness.

2.5 Smart Health Infrastructure:

Integrating IoT into healthcare infrastructure can lead to smart hospitals and clinics, where devices communicate to optimize patient care and resource allocation. Integrating I-Body into healthcare infrastructure transforms facilities into smart environments. Devices communicate seamlessly, leading to more efficient patient care, resource allocation, and overall operational improvements.

2.6 Wearable Technology Integration:

Increasing integration of health monitoring features into everyday wearables for continuous, unobtrusive health tracking. I-Body ensures a seamless integration of health monitoring features into everyday wearables. This integration enhances user experience, making health tracking more unobtrusive and accessible.

2.7 Global Health Connectivity:

Establishing a globally connected network of health monitoring systems facilitates information sharing, aiding in the management of global health challenges. Through I-Body, a globally connected network emerges, facilitating the exchange of health information. This interconnected system aids in addressing global health challenges more effectively through collaborative efforts and shared insights.

III. RELATED WORK

In this section, we exemplify various threats to IoT-based health monitoring system:

3.1 Security Vulnerabilities:

IoT devices may be susceptible to cybersecurity threats, including unauthorized access, data breaches, and malicious attacks, compromising patient confidentiality and system integrity.

3.2 Data Privacy Concerns:

The collection and transmission of sensitive health data raise privacy issues. Inadequate data protection measures may result in unauthorized access, leading to breaches of patient privacy.

3.3 Interoperability Challenges:

Integrating diverse IoT devices and platforms may pose interoperability challenges, hindering seamless communication and data exchange among different components of the health monitoring system.

3.4 Device Malfunctions:

Technical failures or malfunctions of IoT devices, such as sensors or communication modules, could disrupt the continuous monitoring process, affecting the reliability of health data.

3.5 Network Issues:

Reliance on network connectivity for data transmission makes the system susceptible to disruptions, delays, or outages, impacting the real-time monitoring capabilities of the health system.

3.6 Data Accuracy and Integrity:

Inaccurate sensor readings or data manipulation could lead to incorrect health assessments, potentially causing misdiagnoses or inappropriate medical interventions.

IV. A PATIENT MONITORING SYSTEM UTILIZING THE INTERNET OF THINGS FOR REAL TIME TRACKING AND OBSERVATION:

Introduced a real-time tracking system designed to assist in intensive care units (ICUs). The system integrates data from body sensors, utilizing Arduino Uno, and transfers it to a dedicated application. This application facilitates the monitoring of specific parameters within a defined range and connectivity. Leveraging IoT Cloud and protocols, the system enables diverse data transmission ranges to the associated application.

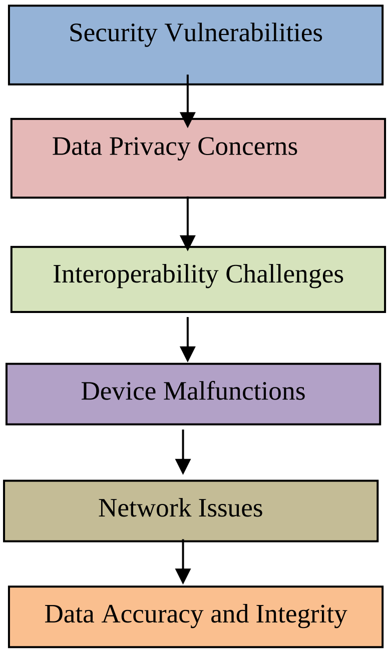


Fig. 2. Threats to IoT-Based Health Monitoring System

V. PROPOSED WORK

We propose the following security methods to mitigating health monitoring system in IoT:

5.1 Secure Authentication:

Utilize robust authentication mechanisms for both devices and users to prevent unauthorized access and ensure only authorized individuals can interact with the system.

5.2 Interoperability Standards:

Adhere to established interoperability standards to ensure seamless communication and integration between different components of the health monitoring system.

5.3 Continuous Monitoring of System Health:

Implement real-time monitoring of the health monitoring system itself to promptly detect and address any anomalies or security breaches.

5.4 Securing IoT Technologies:

Various protocols need to developed, tested and implemented regularly. Probabilistic logic is be implemented while framing the protocols.

5.5 Privacy by Design:

Integrate privacy considerations into the system design phase, emphasizing data minimization, purpose limitation, and user consent to address data privacy concerns.

5.6 Redundancy and Backup Systems:

Establish redundancy and backup mechanisms to ensure the availability and continuity of health monitoring services in the event of device malfunctions or network issues.

5.7 Compliance with Regulations:

Stay abreast of and comply with relevant healthcare regulations, data protection laws, and industry standards to maintain legal and ethical practices.

The Blood Pressure Detector is a non-invasive device specifically created for measuring human blood pressure. Utilizing the oscillometric method, it gauges systolic, diastolic, and mean arterial pressure. These devices function by inflating a cuff, briefly interrupting blood flow through the brachial artery. [5]

Algorithm:

1. Begin
2. Identify Potential threats that could harm in IoT.
3. Focus on the Most Probable Threats that could the resources of IoT.
4. Determine various Security Measures to Protect Resources of IoT.
5. Implement Measures Protect Resources of IoT.
6. Assess the Level of Security implemented in IoT to Prevent Unauthorized Access.
7. End

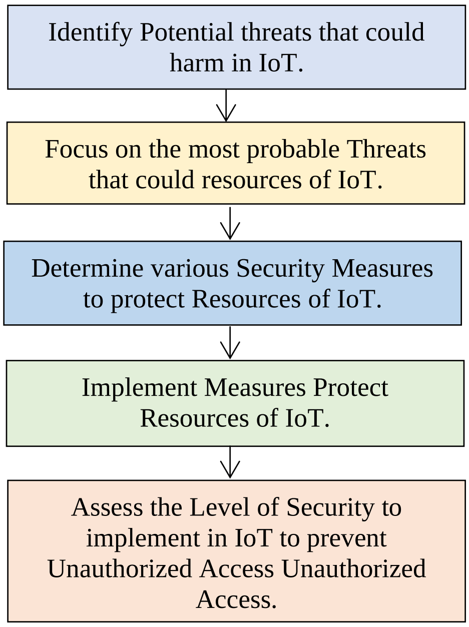

Identify Potential threats that could harm in IoT.
Focus on the most probable Threats that could resources of IoT.
Determine various Security Measures to protect Resources of IoT.
Implement Measures Protect Resources of IoT.
Assess the Level of Security to implement in IoT to prevent Unauthorized Access Unauthorized Access.

Fig. 3. Procedure to safeguard the IoT from various

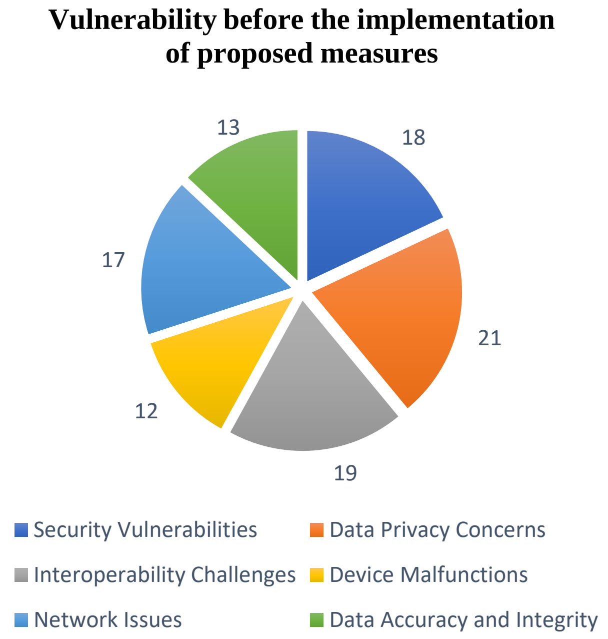


Fig. 4. Vulnerability before following proposed security Measures

VI. RESULT & ANALYSIS

S.No	Types of Attacks Possible on IoT Based Health Monitorizing System	Percentage of Vulnerability
1	Security Vulnerabilities	18
2	Data Privacy Concerns	21
3	Interoperability Challenges	19
4	Device Malfunctions	12
5	Network Issues	17
6	Data Accuracy and Integrity	13
Vulnerability before the implementation of Proposed Security Measures		100
Table 1. Types of Possible Attacks on IoT- Based Health Monitoring System		

S.No	Types of Attacks Possible on IoT Based Health Monitorizing System	Percentage of Vulnerability
1	Security Vulnerabilities	5
2	Data Privacy Concerns	3.2
3	Interoperability Challenges	2.8
4	Device Malfunctions	3
5	Network Issues	6.7
6	Data Accuracy and Integrity	4.3
Vulnerability after the implementation of Proposed Security Measures		25
Table 1. Types of Possible Attacks on IoT- Based Health Monitoring System		

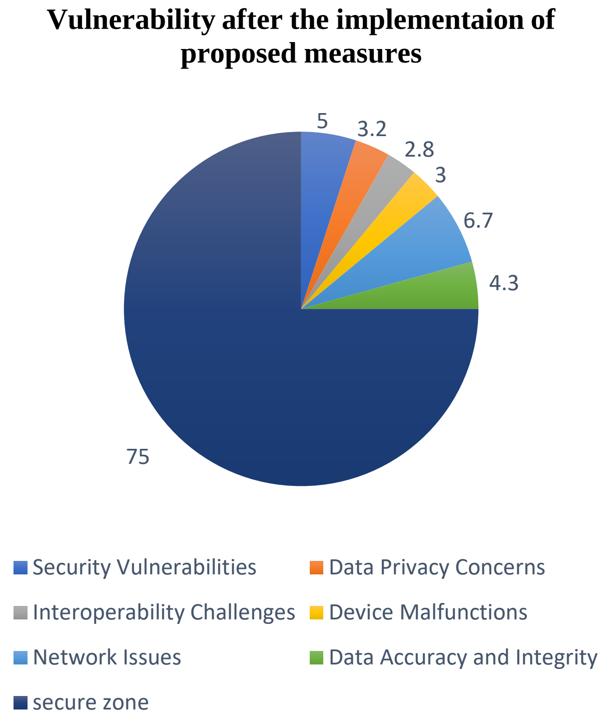


Fig. 5. Vulnerability before following proposed security Measures

VII. CONCLUSION

The IoT-based health monitoring system proves to be a transformative solution, seamlessly integrating technology into healthcare. Its real-time data collection, remote monitoring capabilities, and data analytics contribute to more proactive and personalized patient care. This system not only enhances patient outcomes but also streamlines healthcare processes, ultimately ushering in a new era of efficient and patient-centric healthcare delivery.

VIII. FUTURE

IoT-based health monitoring systems could focus on refining sensor technologies to enhance data accuracy and reliability. Additionally, the integration of advanced machine learning algorithms could enable predictive analytics for early detection of health issues. Exploring interoperability standards to ensure seamless communication between diverse devices and platforms is crucial. Furthermore, addressing cybersecurity concerns to safeguard sensitive health data remains an ongoing priority. Collaborative efforts with healthcare professionals, engineers, and policymakers will be essential for shaping the future evolution of IoT in healthcare.

IX. REFERENCES

[1] A. Sharma, A. K. Sing, K. Saxena, and M. A. Bansal, “Smart health monitoring system using IoT,” International Journal for Research in Applied Science and Engineering Technology, vol. 8, no. 5, pp. 654–658, 2020.

[2] https://ieeexplore.ieee.org/document/9441874

[3] Minnesota Department of Health, “Pulse oximetry and COVID-19,” 2020.

[4] E. C. E. H. A.-I. M. A. N. T. N. C. S. M. &. F. S. Rachkidi, "Towards efficient automatic scaling and adaptive cost-optimized ehealth services in cloud," in In 2015 IEEE global communications conference (GLOBECOM) ,2015.

[5]Dr. D. Y. Patil Institute of Technology https://engg.dypvp.edu.in/blogs/iot-based-health-monitoring-system.

[6] A. A. a. P. M. S. Tyagi, "A conceptual framework for IoT-based healthcare system using cloud computing," in 6th International Conference - Cloud System and Big Data Engineering (Confluence), 2016.

[7] Majer, L., Stopjaková, V., Vavrinský, E.: Sensitive and Accurate Measurement Environment for Continuous Biomedical Monitoring using Microelectrodes. In: Measurement Science Review. - ISSN 1335- 8871. - Vol. 7, Section 2, No. 2 (2007), s. 20-24.

[8] Warsuzarina Mat Jubadi, Siti Faridatul Aisyah Mohd ahak”, Heartbeat Monitoring Alert via SMS”, 978-1-4244-4683-4/09/$25.00 ©2009 IEEE.

[9] Dave Grundgeiger, Programming Visual Basic.Net, First Edition 2002, O’Reilly Publication, ISBN: 0- 596-00093-6, 464 Pages.

[10] T. E. Dietz and P. H. Hackett, "High-Altitude Medicine" in Travel Medicine, Elsevier, pp. 387-400, 2019.

[11] Aleksander Kotevski, Natasa Koceska and Saso Koceski, "E-health Monitoring System", International Conference on Applied Internet and Information Technologies, 2016.

Video Shot Boundary Detection Using Principal Component Analysis (PCA) and Deep Learning

RASANI SUNANDINI
23DSC13, M.Sc (Computational Data Science)
Department of computer science
P.B.Siddharatha College of Arts & Science
Vijayawada, A.P, India
rasanisunandini@gmail.com

SEEPANA NANDINI
23DSC18, M.Sc (Computational Data Science)
Department of computer science
P.B.Siddharatha College of Arts & Science
Vijayawada, A.P, India
nandiniseepana111@gmail.com

BORA UMA REDDY
23DSC21, M.Sc (Computational Data Science)
Department of computer science
P.B.Siddharatha College of Arts & Science
Vijayawada, A.P, India
Umakrishna7620@gmail.com

ABSTRACT: In the Aftermath of the COVID-19 Pandemic, The Global Surge in Reliance on Digital Media Platforms Has Underscored the Significance of Advanced Video Surveillance, Video Content Analysis, And Video Retrieval Tasks. Traditional Methods for Shot Boundary Detection (SBD) Face Challenges, Particularly in Identifying Gradual Transition Types of Shot Boundaries. SBD Serves as A Crucial Initial Step in Video Processing, Facilitating the Segmentation of Video Sequences into Distinct Shots. Large-Scale Videos Encompass Diverse Shot Transitions, Including Gradual and Cut Variations. Achieving Higher Accuracy in Detecting These Transitions Demands an Efficient SBD Method. While Prior Researchers Have Proposed SBD Methods Employing Supervised Machine Learning Approaches, The Limitation of Data Availability for Training Poses A Constraint. Unsupervised Approaches Have Also Been Explored in Previous Literature; However, They Often Fall Short in Accurately Detecting Gradual Transition Shot Boundaries. This Paper Introduces an Innovative Approach To SBD, Utilizing A Distance Calculating Algorithm Based on Principal Component Analysis (PCA) Features and Complementing it with A Deep Learning Method to Enhance Precision in Detecting Gradual Transition Shot Boundary Frames and Normal Frames. The Proposed Methodology Involves the Following Steps: First, PCA Is Applied for Feature Extraction from Video Frames, Wherein the Most Significant Eigenvectors and Eigenvalues Are Analyzed. Subsequently, A Distance Calculating Algorithm Is Employed on Adjacent Video Frames, Leveraging Their Eigenvectors and Eigenvalues to Ascertain Shot Boundaries. To Further Refine Detection Accuracy, False Detection Boundaries Are Scrutinized and Classified Using Convolutional Neural Networks (CNN). Experimental Results Demonstrate the Efficacy of The Proposed Method, Showcasing Its Ability to Improve the Precision of Gradual Transition Shot Boundary Detection.

KEYWORDS: Shot Boundary Detection, Sbd, Video Analysis, PCA, Deep Learning, Cnn, Distance Calculation, Video Processing.

I. INTRODUCTION

Shot Boundary Detection (SBD) stands as a fundamental and crucial initial phase in video processing and analysis, playing a pivotal role in the operations of intelligence agencies and businesses alike. Intelligence agencies leverage video processing for tasks such as video concept analysis and semantic interpretation of intricate videos, content-based video browsing, and efficient event retrieval. In the business domain, the ability to discern the type of content an individual is viewing online is harnessed to tailor product offerings, facilitating targeted marketing strategies. This enables business owners to align their products with consumer interests, thereby enhancing sales and engagement depending on their transitions such as cut transition (immediate or abrupt change from one shot to another shot,shown in "Fig. 3") and gradual transition (slow or gradual change from one shot to another shot such as dissolve, wipe, fade in or fade out which is shownin "Fig.4","Fig.5",and"Fig.6").The traditional framework of SBD is as follows(shownin"Fig.1").

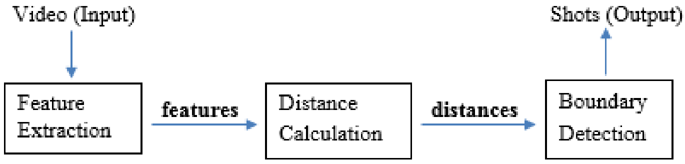


Fig.1.SBDframework

Fig.2.Normalframes

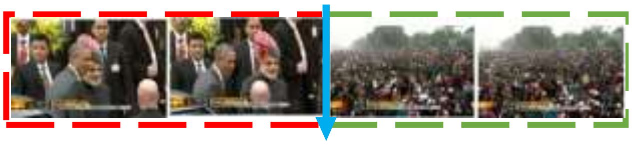


Fig. 3. Cut shot boundary

Shot A Gradual transition shot boundary
Shot B Fig.4. Gradual shot boundary (dissolvetransition)

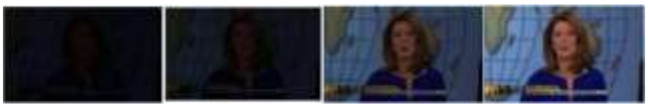
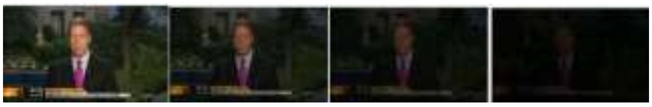


Fig.5. Gradual shot boundary (fade in transition)
Fig.6.Gradual shot boundary (fade out transition)



Feature extraction is an essential step for the SBD framework. The authors of [1] extracted the features based on visually multi-modal features. To do so, they analyzed the behavior of temporal characteristics from visual features, based on SURF (Speeded-Up Robust Features descriptors) and RGB histogram. This method did not perform well for gradual transition type shot boundary detection as compared to the cut type shot boundary detection. This feature extraction technique is unable to extract sufficient features and could not tolerate the disturbances generated by the effect of object movement and background changes. The authors of [4] used DMD (dynamic mode decomposition) for feature extraction which depends on the temporal characteristics. This method is sensitive to brightness changes. Since, in dissolve type gradual transition, the brightness change is very slow, thus this method is unable to provide good detection accuracy for dissolve type gradual transition. Extracting histogram features in HSV (Hue, Saturation, Value) is another method, proposed in [5]. The drawback of their method is they are sensitive to objects' movements due to rapid color changes. The second step of the SBD framework is to calculate the distance between two adjacent frames. There are many novel methods for distance or dissimilarity calculation between two adjacent frames such as Bhattacharya distance [2], Euclidean distance [3]. However, some SBD approaches show that distance calculation may not depend on only one feature due to its trade-off of multiple features, thus some papers used feature weighting based on machine learning such as fuzzy logic [7]. The final step of the SBD framework is shot boundary detection and classification. Some papers proposed statistical machine learning-based approach such as SVM (Support Vector Machine) [8]. SVM classification gives good results but it needs a good balance of the training dataset. The authors of [6] proposed a method to locate shot boundaries using an adaptive threshold. Many unsupervised learning techniques are also proposed [2] [7] to avoid the training process, however, supervised learning works better than unsupervised. The authors of [2] used Canny Edge detection algorithm to review false detection so that SBD precision can be improved. However, this review algorithm is well suited for cut type transition, not for gradual type transition due to the fact that the differences between two adjacent frames are too small in gradual type transition. Even though traditional proposed methods are able to detect cut type transition with high accuracy, most of them are unable to detect gradual type transition (especially dissolve type) with high accuracy. To improve detection precision of gradual type transition, an effective SBD framework is needed. The main contributions of this paper are listed as follows. Features are extracted by using PCA. PCA gives Eigenvectors and Eigenvalues which hold the most significant features of the video frames. After extracting the features, distances are calculated between adjacent frames. This distance calculating algorithm is designed based on some conditions using Eigen vectors and Eigenvalues and then transition (gradual, cut) frames and normal frames (shown in "Fig. 2") are detected. Finally, to improve the precision, CNN (ResNet 50 network) is used to detect false detected transition frames and normal frames and then classifying them in a new transition frames and normal frames.

II. SYSTEM ARCHITECTURE AND PROCESS

The whole process in the system architecture, can be explained in four steps, pre-processing (step 1), PCA (Step 2), distance algorithm and SBD (step 3), and CNN (convolutional neural network) for frame classification (step 4) in "Fig. 7".

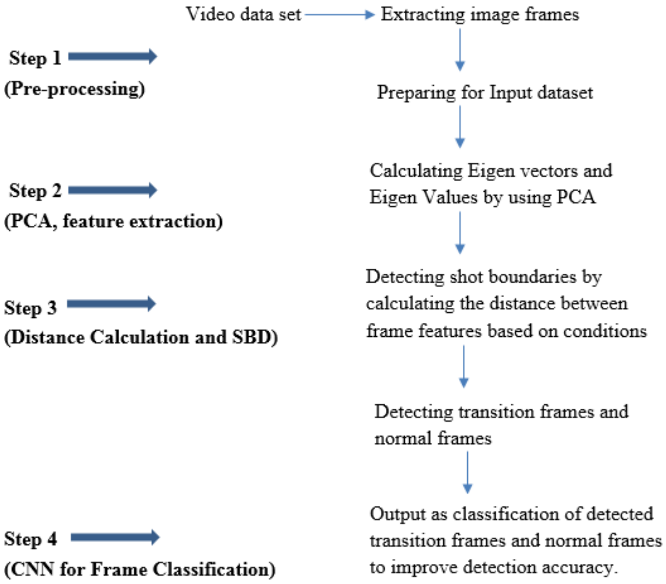

Video data set
Extracting image frames
Step 1
(Pre-processing)
Preparing for Input dataset
Step 2
(PCA, feature extraction)
Calculating Eigen vectors and Eigen Values by using PCA
Step 3
(Distance Calculation and SBD)
Detecting shot boundaries by calculating the distance between frame features based on conditions
Detecting transition frames and normal frames
Step 4
(CNN for Frame Classification)
Output as classification of detected transition frames and normal frames to improve detection accuracy.

Fig.7.Systemarchitecture

The main contribution of this paper lies in steps 1-3 in part1.

A. Step-1 (Pre-processing)

Video frames are extracted from the video data and thereafter, extracted video frames are stored as input dataset to the system. Images are all color images i.e. in RGB. All frames are in the same size i.e. 700x1200x3.

B. Step-2 (PCA, feature extraction)

PCA is applied to the input dataset to calculate the Eigenvalues and Eigenvectors consisting of most of the features of the image frames. After that, the changes of Eigen values and Eigenvectors per video frames are analyzed to understand the co-relation.

C. Step-3 (Distance calculation and SBD)

The distance algorithm is designed based on some conditions to calculate the dissimilarity between video frame's features (shown in Methodology). In a continuous video sequence, the change in video frame features is similar. The inequality occurs when shot boundary occurs between two continuous video sequences, this helps to derive the condition for distance calculations between two adjacent video frames. Using this distance calculating algorithm, the transition frames (gradual, cut) in shot boundaries, and normal frame (non-shot boundary) are detected.

D. Step-4 (CNN for frame classification)

CNN is used to improve the detection accuracy. After performing step-3, the false detected transition (shot) frames and normal(non-shot) frames are fed through CNN for detecting the actual transition and normal frames and then classified them into new transition and normal frames. Experiments show that the above system architecture has improved the detection accuracy for both gradual and cut transition types hot boundaries than the conventional methods.

III. METHODOLOGY

A. Pre-processing

This is an initial step for making the data set to get ready for the further steps, called pre-processing step. A video sequence is basically a stack of image frames that are put together at a continuous signal. The discontinuity between two shots (continuous video sequence) is called shot boundary. To detect shot boundary, a pre-processing step is proposed as the initial step. Firstly, video frames are extracted from the video and stored in a dataset. The further steps are performed on this dataset by loading the dataset in the system.

B. PCA feature extraction

PCA (Principal Component Analysis) is an existing well-known method that can calculate the most significant Eigen vectors and Eigenvalues from an image. In this paper, PCA is used on the video frames to get the Eigenvectors and Eigen values consisting most of the appropriate features of the video frames. These Eigenvalues and Eigenvectors are analyzed for understanding the changes in themfor normal frames and shot boundary frames (Cut transition, gradual transition).

C. Distance calculation and SBD

Shot and non-shot boundaries are detected by using a distance algorithm. This distance algorithm is designed to calculate the distance/dissimilarity by using Eigen values and Eigen vectors between each frame in the video and then some conditions are considered to identify shot and non-shot boundaries. The conditions in the distance algorithm are proposed as follows.

Algorithm: **Distance calculating algorithm**

Notation: D_1, D_2, ……, D_{n-1}, where 'D' denotes the distances between adjacent frames. 'n' denotes number of frames.

F_1, F_2, ……, F_n, where 'F' denotes the feature for 'n' number of frames.

Therefore, $D_1=F_1–F_2$, $D_2=F_2–F_3$……., $D_{n–1}=F_{n-1}–F_n$

Condition1: for normal frames, D_1, D_2……, $D_{n-1}$are approximately equal to Zero.

Condition 2: For Cut shot boundary, If, F_1, F_2, F_3, F_4represent shot A and F_5, F_6, F_7, F_8 represent shot B then, D_1~=D_2~=D_3, D_5~=D_6~=D_7 and D_4 will be in equal. D_4 is where cut shot boundary transition occurred.

Condition3: for gradual dissolve transition shot boundary, If, F_1, F_2, F_3 and F_7, F_8, F_9 represent normal frames and transition occurred in between i.e. F_3, F_4, F_5, F_6, then, D_1~=D_2 and D_3will be inequal; D_7~= D_8, and D_6 will be inequal. Next, normal frames (non-shot boundaries) and transition frames (shot boundaries) for gradual and cut shot type boundaries are classified using CNN.

D. Frame classification using CNN

CNN (ResNet 50 network) is used for reviewing the false detected shot and non-shot boundaries and classifying them in two classes i.e. normal frames and transition frames. This step improves the detection accuracy, hence holds an important step in the proposed method.

IV. EXPERIMENTAL RESULT AND DISCUSSION

The video dataset includes news reports and sports. It contains 41360 image frames and 174 shots. The videos are downloaded from online sources and then processed for input dataset. Some video frames are shown in Table I., where each video frame represents a sequence of the video dataset. The proposed method has focused on detecting cut shot boundary and gradual transition (dissolve, fade in, fade out) shot boundary. The number of frames per second is 24 – 30.

TABLE I: VIDEO DATASET

Genre	Sequences		
News report			
Sports			

The experimental results are shown in three steps. The first step is feature extraction. Features from the input image data set are extracted using PA and then Eigenvectors and Eigenvalues of image frames are analyzed. A comparison table in accuracy for feature extraction is shown below.

TABLE II: FEATURE EXTRACTION COMPARISION

Parameter	Methods		
	HSV	***RGB***	***PCA***
Accuracy	94.5%	93%	95%

In the second step, After PCA features extraction, dissimilarity between adjacent frames is found by using distance calculation algorithm. The distances are calculated using co- relation between Eigenvalues and Eigen vectors. A graphical representation of the distances between adjacent frames with the number of games is provided below for cut and graduation transition (dissolve) type shot boundary.

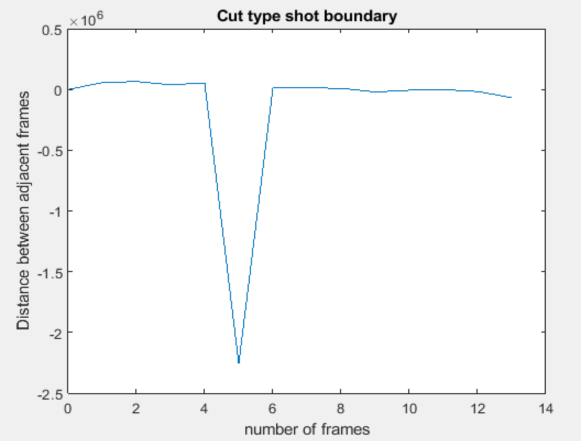


Fig.8.Cutshotboundary

In the “Fig.8”, the minimum peak represents cut shot boundary(discontinuity) between two video sequences.

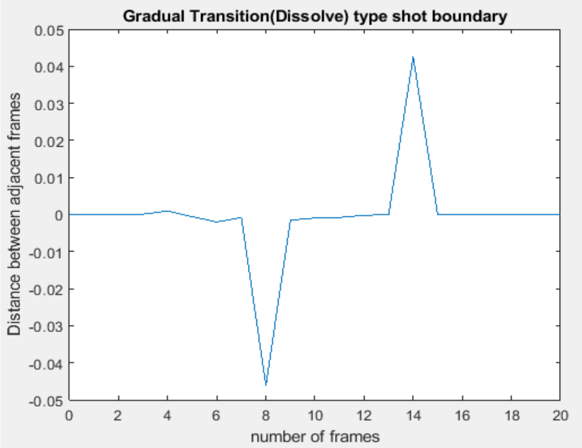


Fig.9.Gradual shot boundary (dissolve transition)

In “Fig. 9”, the minimum peak represents where gradual transition started and the maximum peak represents where gradual transition ends. The saturation denotes distance between normal frames.

TABLE III: DISTANCE CALCULATION COMPARISION

Parameter	Methods		
	Bhattacharya	***Chi-square***	***Our algorithm***
Accuracy	99.91%	99.29%	89.3%

Table III represents comparison in accuracy for distance calculation between traditional methods (Bhattacharya, Chi- square) and our method. To improve detection accuracy, false detected frames are fed through CNN (ResNet 50 network) and then classified between normal frames and gradual transition frames.

TABLE IV: SHOTBOUNDARYDETECTION

Actual number of shots		**Detected number of shots**	
Cut	Gradual	Cut	Gradual
113	61	110	55

The numbers of detected cut and gradual transition shot boundaries are shown in Table IV. The overall accuracy of our method is 97.34% (cut shot boundary) and 90.01% (gradual transition shot boundary in dissolve, fade in and fade out), which shows the effectiveness of our method.

V. CONCLUSION

This paper proposes a PCA feature and deep learning-based SBD method, in which consideration is given to both accuracy and efficiency. Even though our distance calculating algorithm gives less accuracy than traditional method, the overall accuracy for Cut and gradual transition shot boundary detection is improved after using CNN frame classification.

For future work, proposed method will be improved to detect mix shot boundaries and semantically related shots.

VI. REFERENCES

[1] S. Tippaya, S. Sitjongsataporn, T. Tan, M. M. Khan and K. Chamnongthai, "Multi-Modal Visual Features-Based Video Shot Boundary Detection," in IEEE Access, vol. 5, pp. 12563-12575, 2017, doi:10.1109/ACCESS.2017.2717998.G.

[2] N. Su, J. Zhang, Y. Zhang and G. Zhang, "Unsupervised Clustering Based Real-time Shot Boundary Detection for Live Broadcasting," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 135-140, doi:10.1109/ICCC47050.2019.9064356.

[3] L. Wu, S. Zhang, M. Jian, Z. Lu and D. Wang, "Two Stage Shot Boundary Detection via Feature Fusion and

Spatial-Temporal Convolutional Neural Networks," in IEEE Access, vol. 7, pp. 77268-77276, 2019, doi: 10.1109/ACCESS.2019.2922038.

[4] C. Bi et al., "Dynamic Mode Decomposition Based Video Shot Detection," in IEEE Access, vol. 6, pp. 21397-21407, 2018, doi:10.1109/ACCESS.2018.2825106.

[5] Y. Gao, Y. Lai and Y. Liu, "Fast Video Shot Boundary Detection Based on Visual Perception," 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-4, doi:10.1109/ICCE.2019.8662083.

[6] J. Xu, L. Song and R. Xie, "Shot boundary detection using convolutional neural networks," 2016 Visual Communications and Image Processing (VCIP), Chengdu, China, 2016, pp. 1-4, doi:10.1109/VCIP.2016.7805554.

[7] Xinbo Gao and Xiaoou Tang, "Unsupervised video-shot segmentation and model-free anchor person detection for news video story parsing," in IEEE Transactions on Circuits and Systems for Video Technology, vol.12, no. 9, pp. 765-776, Sept. 2002, doi: 10.1109/TCSVT.2002.800510.

[8] Yongliang Xiao, "An effective video shot boundary detection method based on supervised learning," 2010 2nd International Conference on Advanced Computer Control, Shenyang, China, 2010, pp. 371-374, doi:10.1109/ICACC.2010.5486933.

Network Slicing in 5G

A.PHANI KUMAR
22MCA28, M.C.A
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, AP, India
karrilokesh150@gmail.com

CH.DINESH
22MCA36, M.C.A
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, AP, India
chintapallidinesh8824@gmail.com

K.LOKESH
22MCA29, M.C.A
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, AP, India
phanikumaralthi164@gmail.com

ABSTRACT: As the Telecommunications Landscape Evolves with The Advent Of 5G Technology, The Concept of Network Slicing Emerges as A Pivotal Architectural Innovation. This Article Delves into The Transformative Potential of Network Slicing, Offering A Comprehensive Exploration of Its Technical Underpinnings, Challenges, And Diverse Applications. Network Slicing Enables the Creation of Isolated and Customized Virtual Networks Tailored to Specific Service Requirements, Ranging from Enhanced Mobile Broadband to Ultra-Reliable Low-Latency Communication and Massive Machine-Type Communication. The Paper Addresses the Critical Components of Network Slicing, Including Resource Isolation, Orchestration, And Dynamic Scaling. It Also Investigates Challenges Such as Security, Inter-Slice Communication, And Resource Optimization, Presenting Viable Solutions. Through Case Studies, The Article Showcases Successful Implementations of Network Slicing, Illustrating Its Tangible Impact on Service Quality and Efficiency. Looking Forward, The Discussion Extends to Future Directions, Including the Integration of Network Slicing with Emerging Technologies and its Evolution in Subsequent Generations of Wireless Networks. This Article Serves as A Comprehensive Resource for Researchers, Practitioners, And Industry Professionals Seeking to Understand, Implement, And Contribute to the Evolution of Network Slicing in 5G Networks and Beyond.

KEYWORDS: Network Slicing, 5G, Enhanced Mobile Broadband (Embb), Ultra-Reliable Low Latency Communication (URLLC), Massive Machine Type Communication (Mmtc), Quality of Service (Qos), Edge Computing, Industry 4.0.

I. INTRODUCTION

The advent of 5G technology represents a paradigm shift in the telecommunications landscape, ushering in an era of unprecedented connectivity and technological innovation. At the heart of this transformative wave lies the concept of network slicing, a groundbreaking architectural framework poised to redefine the capabilities and flexibility of wireless networks. Network slicing empowers service providers to partition their infrastructure into isolated and customizable virtual networks, each tailored to meet the unique demands of diverse applications and services. A major concern in adaptation of cloud for data is security and privacy [4]. It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data. This article navigates through the intricacies of network slicing within the 5G ecosystem, aiming to provide a thorough understanding of its technical foundations, challenges, and the myriad applications it enables. As 5G networks strive to accommodate an increasingly diverse set of services from enhanced mobile broadband to ultra-reliable low-latency communication and massive machine-type communication the need for a flexible and efficient network infrastructure becomes paramount. Network slicing emerges as the linchpin that facilitates this dynamic adaptation, allowing for the simultaneous coexistence of disparate services on a shared physical infrastructure. In this introductory section, we set the stage by offering a brief overview of 5G technology and highlighting the compelling need for network slicing. As we delve into the technical intricacies, challenges, and applications of network slicing in subsequent sections, it becomes evident that this concept is not merely an incremental enhancement but a foundational shift in the way we conceptualize and implement wireless communication networks. Through a comprehensive exploration of network slicing, this article aims to contribute to the ongoing discourse surrounding the evolution of 5G networks, providing insights for researchers, practitioners, and industry stakeholders alike.

II. TECHNICAL FOUNDATIONS OF NETWORK SLICING

The successful implementation of network slicing within 5G networks relies on a robust technical foundation that encompasses the architecture, key components, and operational principles. This section elucidates the core technical aspects that underpin network slicing, facilitating an in-depth understanding of its mechanisms.

A. 5G Network Architecture:

The architecture of 5G networks forms the bedrock for the realization of network slicing. It comprises three primary components: The User Equipment (UE), the Radio Access Network (RAN), and the 5G Core (5GC). The flexibility and adaptability of 5G architecture allow for the effective deployment and orchestration of network slices.

B. Core Components of Network Slicing:

i. Slice Management and Orchestration:

Network slicing necessitates a robust management and orchestration layer that dynamically allocates resources and configures network functions. This involves the instantiation, monitoring, and scaling of slices to accommodate varying service requirements.

ii. Virtualization Technologies:

Virtualization technologies, including Network Function Virtualization (NFV) and Software-Defined Networking (SDN), play a pivotal role in the realization of network slicing. NFV enables the virtualization of network functions, while SDN provides programmability and flexibility in managing network resources.

iii. Resource Isolation:

Ensuring the isolation of resources between different network slices is crucial to prevent interference and maintain the integrity of services. Techniques such as network slicing-aware radio resource management are employed to optimize resource allocation for each slice.

iv. Dynamic Scaling and Flexibility:

Network slicing offers dynamic scaling capabilities to adapt to fluctuating demands. Through automated processes, slices can scale resources up or down based on real-time requirements, ensuring efficient resource utilization and optimal performance.

v. End-to-End Network Slicing:

Network slicing spans the entire network, encompassing both the radio and core network segments. This end-to-end approach ensures that the benefits of slicing, including low latency and high throughput, are realized consistently across all network components.

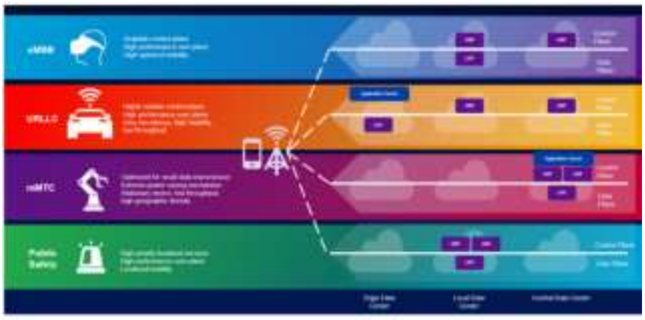
vi. Network Slicing and Quality of Service (QoS):

Quality of Service is a critical consideration in network slicing. Each slice is configured to meet specific QoS parameters, guaranteeing the required level of performance for the associated services. This involves the allocation of bandwidth, latency control, and reliability management.

In summary, the technical foundations of network slicing in 5G networks encompass a dynamic and flexible architecture, virtualization technologies, resource isolation, and end-to-end orchestration. Understanding these core components is essential for unlocking the full potential of network slicing and tailoring network infrastructures to the diverse requirements of modern applications and services.

III. TYPES OF NETWORK SLICES

Network slicing introduces a versatile framework that allows the creation of tailored virtual networks to cater to specific service requirements. These slices are designed to meet the unique demands of diverse applications, providing a customizable and efficient approach to network deployment within the 5G ecosystem.



1) Enhanced Mobile Broadband (eMBB) Slices:

eMBB slices are engineered to deliver high data rates and increased capacity, catering to applications demanding enhanced mobile connectivity. These slices are ideal for services such as high-definition video streaming, virtual reality (VR), and augmented reality (AR) applications, ensuring a seamless and immersive user experience.

2) Ultra-Reliable Low Latency Communication (URLLC) Slices:

URLLC slices prioritize ultra-reliable communication with minimal latency, making them suitable for mission-critical applications. This includes services like autonomous vehicles, industrial automation, and remote surgery, where instantaneous response times and high reliability are paramount for safe and efficient operations.

3) Massive Machine Type Communication (mMTC) Slices:

mMTC slices are tailored to accommodate a massive number of devices simultaneously, making them suitable for applications characterized by a vast number of connected devices. Examples include smart cities, smart agriculture, and the Internet of Things (IoT) deployments, where scalability and efficient handling of numerous low-power devices are crucial.

4) Customized Slices for Specific Industries:

Network slicing allows for the creation of slices customized to the unique needs of specific industries. This includes sectors such as healthcare, manufacturing, and transportation, where bespoke network configurations can optimize connectivity to address industry-specific challenges and requirements.

Healthcare Slices: Designed to support telemedicine, remote patient monitoring, and other healthcare applications with stringent data security and low-latency requirements.

Manufacturing Slices: Optimized for the connectivity needs of smart factories, supporting real-time communication for industrial automation, robotics, and quality control systems.

Transportation Slices: Tailored for connected and autonomous vehicles, enabling low-latency communication and high-reliability connectivity for navigation, traffic management, and safety applications.

5) **Dynamic Slices for Evolving Services:**
Network slicing enables the creation of dynamic slices that can adapt to changing service requirements. This flexibility allows for the seamless deployment of new services and applications without significant infrastructure modifications.

In summary, the categorization of network slices into eMBB, URLLC, mMTC, industry-specific slices, and dynamic slices showcases the versatility of network slicing in addressing the diverse needs of applications and industries within the 5G ecosystem.

IV. CHALLENGES AND SOLUTIONS

The implementation of network slicing in 5G networks introduces several challenges that need to be addressed to ensure the seamless operation and optimization of this innovative framework. This section outlines key challenges and proposes viable solutions to overcome them.

A. Security Challenges:

i. **Isolation of Slice Traffic:**
Challenge: Ensuring secure isolation between different network slices to prevent unauthorized access and potential data breaches.
Solution: Implement robust encryption protocols and secure virtualization techniques to guarantee the integrity and confidentiality of data within each slice.

ii. **Inter-Slice Security:**
Challenge: Managing security across multiple slices and preventing potential vulnerabilities in inter-slice communication.
Solution: Employ advanced security mechanisms, such as intrusion detection systems and secure communication protocols,to safeguard interactions between different slices.

B. Resource Allocation and Optimization:

i. **Dynamic Resource Management:**
Challenge: Efficiently allocating resources to slices in real-time to meet varying demands and prevent resource contention.
Solution: Implement dynamic resource management algorithms that adapt to changing network conditions and prioritize resource allocation based on slice requirements.

ii. **Slice Scaling and Mobility:**
Challenge: Enabling dynamic scaling of slices and seamless mobility of devices across slices without compromising performance.
Solution: Implement automated scaling mechanisms that can dynamically adjust resources based on demand and ensure continuous connectivity during device mobility.

C. Inter-Slice Communication:

i. **Coexistence of Diverse Slices:**
Challenge: Facilitating effective communication between slices while maintaining the isolation required for each.
Solution: Implement standardized communication interfaces and protocols, ensuring compatibility and secure interaction between different slices.

ii. **Orchestration Complexity:**
Challenge: Managing the orchestration of diverse slices without introducing complexity and inefficiency.
Solution: Develop advanced orchestration frameworks that streamline the deployment and management of slices, automating processes to minimize complexity.

D. Slice Lifecycle Management:

i. **Dynamic Slice Instantiation:**
Challenge: Enabling rapid and on-demand instantiation of slices to accommodate varying service requirements.
Solution: Implement efficient slice lifecycle management systems that can dynamically create, modify, and terminate slices based on demand.

ii. **Slice Monitoring and Analytics:**
Challenge: Monitoring the performance of individual slices and collecting actionable analytics to optimize resource utilization.
Solution: Deploy monitoring tools and analytics platforms that provide real-time insights into slice performance, facilitating proactive adjustments and optimizations.

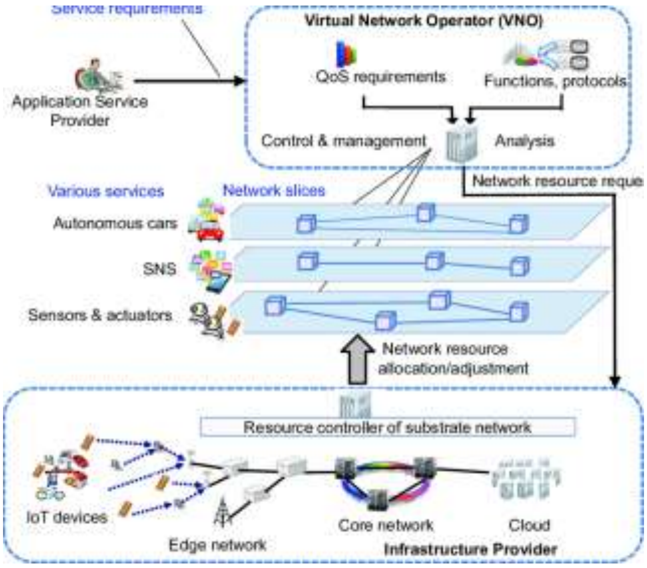
E. Standards and Interoperability:

i. **Lack of Standardization:**
Challenge: The absence of standardized interfaces and protocols may hinder interoperability between network elements and limit the widespread adoption of network slicing.
Solution: Engage in collaborative efforts to establish industry-wide standards for network slicing, fostering interoperability and seamless integration across different network infrastructures.

In addressing these challenges, network operators and researchers can pave the way for the widespread deployment of network slicing in 5G networks, ensuring the realization of its full potential in providing customized, efficient, and secure connectivity for diverse applications and services.

V. APPLICATIONS OF NETWORK SLICING

Network slicing opens the door to a multitude of applications, each tailored to specific needs and characteristics. This section explores how network slicing can be applied across various sectors to enhance services, optimize performance, and meet the diverse requirements of modern applications.



A. **Improved Quality of Service (QoS) for Specific Applications:**

i. **Video Streaming and Enhanced Media Delivery:**

Application: eMBB slices ensure high data rates and low latency, providing an optimal environment for high-definition video streaming and enhanced media delivery.

ii. **Gaming and Augmented/Virtual Reality (AR/VR):**

Application: eMBB and URLLC slices cater to low-latency and high-throughput requirements, enhancing the gaming experience and supporting AR/VR applications.

B. **Edge Computing and Network Slicing Synergy:**

i. **Smart Cities and IoT Deployments:**

Application: The mMTC slice is designed for massive device connectivity, supporting smart city initiatives, and large-scale Internet of Things (IoT) deployments.

ii. **Real-time Industrial Automation:**

Application: URLLC slices enable real-time communication for industrial automation, supporting robotics and manufacturing processes.

C. **Industry-Specific Use Cases:**

i. **Connected and Autonomous Vehicles:**

Application: Dedicated slices ensure low-latency communication, supporting reliable and secure connectivity for connected and autonomous vehicles.

ii. **Healthcare Applications:**

Application: Customized slices address the stringent requirements of healthcare applications, such as telemedicine and remote patient monitoring, ensuring data security and low latency.

iii. **Smart Agriculture:**

Application: mMTC slices accommodate a vast number of low-power devices in smart agriculture applications, optimizing resource usage and scalability.

D. **Public Safety and Emergency Services:**

i. **Emergency Response and Disaster Management:**

Application: URLLC slices provide the low-latency and high-reliability communication required for emergency response and disaster management systems.

E. **Dynamic Slices for Evolving Services:**

i. **Internet of Things (IoT) Evolution:**

Application: Dynamic slices accommodate the evolving landscape of IoT services, allowing for the seamless integration of new devices and applications.

ii. **5G Evolution and Beyond:**

Application: Dynamic slices facilitate the smooth transition to future generations of wireless networks, supporting the evolution of technology beyond 5G.

In summary, the applications of network slicing are vast and diverse, catering to specific service requirements across industries. From enhancing the quality of multimedia applications to enabling real-time industrial automation and supporting critical services like healthcare and emergency response, network slicing proves to be a versatile and powerful tool in shaping the future of connected services.

VI. CASE STUDIES

Case studies provide real-world examples that showcase the practical implementation and impact of network slicing in diverse scenarios. The following case studies illustrate successful instances where network slicing has been employed to address specific challenges and enhance services.

A. Enhanced Mobile Broadband (eMBB) for High-Speed Connectivity:

Case Study: Augmented Reality Streaming

In a metropolitan area, an eMBB network slice was deployed to support an augmented reality (AR) streaming service. Users experienced seamless and high-quality AR content delivery with minimal latency. The eMBB slice optimized data rates, ensuring an immersive and real-time AR experience for users in crowded urban environments.

B. Ultra-Reliable Low Latency Communication (URLLC) for Industrial Automation:

Case Study: Smart Manufacturing

In a smart manufacturing facility, a URLLC network slice was implemented to support real-time communication between industrial robots and control systems. The URLLC slice ensured ultra-reliable connectivity, enabling precise and instantaneous control over robotic operations. This resulted in increased efficiency and reduced latency in the manufacturing processes.

C. Massive Machine Type Communication (mMTC) for IoT Deployments:

Case Study: Smart Agriculture

In a large-scale agricultural setting, an mMTC network slice was tailored to accommodate a multitude of sensors and devices for smart farming. The slice efficiently managed data from various agricultural sensors, enabling farmers to monitor soil conditions, crop health, and automate irrigation. The mMTC slice enhanced scalability and resource utilization in the agricultural IoT ecosystem.

D. Customized Slices for Healthcare Applications:

Case Study: Telemedicine Network Slice

In a healthcare network, a customized network slice was dedicated to telemedicine applications. The slice ensured low-latency, secure, and reliable communication between healthcare providers and patients. This facilitated remote consultations, real-time monitoring, and timely access to medical information, contributing to improved patient care and healthcare accessibility.

E. Dynamic Slices for Evolving Services:

Case Study: IoT Evolution in Smart Cities

In a smart city deployment, dynamic network slices were utilized to accommodate the evolving landscape of IoT devices. As new sensors and applications were introduced, the dynamic slices seamlessly adapted to the changing demands. This facilitated the integration of smart transportation, waste management, and public safety services, showcasing the scalability and flexibility of network slicing.

These case studies highlight the versatility and effectiveness of network slicing in addressing specific use cases across different industries. Whether optimizing connectivity for augmented reality, ensuring ultra-reliable communication in industrial settings, supporting massive IoT deployments in agriculture, tailoring slices for healthcare applications, or adapting to the dynamic nature of smart cities, network slicing proves to be a powerful tool for enhancing services and meeting the unique requirements of diverse applications.

VII. FUTURE DIRECTIONS

The evolution of network slicing in 5G networks opens the door to numerous opportunities and challenges. As technology continues to advance, several future directions emerge, shaping the trajectory of network slicing and its applications. The following areas represent key aspects that researchers and industry professionals should explore in the years ahead:

A. Integration with Emerging Technologies:

i. Artificial Intelligence (AI) and Machine Learning:

Investigate how AI and machine learning algorithms can be integrated into network slicing orchestration and management to enhance resource allocation, predictive maintenance, and automated decision-making.

ii. Blockchain Technology:

Explore the use of blockchain to enhance the security and trustworthiness of network slices, ensuring transparent and tamper-resistant management of network resources and transactions.

B. Network Slicing Beyond 5G:

i. 6G and Beyond:

Anticipate the role of network slicing in future wireless communication standards, such as 6G, and investigate how it can evolve to meet the requirements of increasingly sophisticated applications and services.

ii. Terahertz (THz) Communication:

Examine the feasibility and potential of network slicing in the context of emerging THz communication technologies, addressing challenges related to spectrum utilization and propagation characteristics.

C. Customization for Industry Verticals:

i. Cross-Industry Collaboration:

Foster collaboration between telecommunication providers and industries to tailor network slices specifically for verticals such as energy, manufacturing, and transportation, ensuring the seamless integration of 5G capabilities into diverse ecosystems.

ii. Standardization and Interoperability:

Advocate for continued standardization efforts to ensure interoperability between different network slices, allowing for seamless communication and service delivery across diverse industry sectors.

D. Security and Privacy Enhancements:

i. Zero-Trust Security Models:

Explore and implement zero-trust security models within network slicing architectures to mitigate evolving cyber threats, ensuring a robust and secure environment for diverse applications.

ii. Privacy-Preserving Techniques:

Investigate privacy-preserving techniques within network slicing, focusing on methods to anonymize and protect user data while maintaining the required levels of service quality.

E. Sustainable and Green Networking:

i. Energy-Efficient Slicing:

Develop energy-efficient network slicing strategies to minimize the environmental impact of 5G networks, considering the growing demand for sustainability and green networking.

ii. Dynamic Resource Optimization:

Investigate dynamic resource optimization techniques that consider both performance requirements and energy efficiency, ensuring a balance between quality of service and environmental sustainability.

F. Edge Computing Integration:

i. Edge-Enabled Slices:

Explore the integration of edge computing resources with network slices, enabling low-latency and high-throughput services at the network edge, particularly for latency-sensitive applications.

ii. Federated Learning in Edge Slices:

Investigate the potential of federated learning within edge slices, allowing for collaborative model training without compromising data privacy, particularly relevant for AI-driven applications.

As network slicing continues to mature, these future directions present exciting avenues for innovation and research, ultimately shaping the next phases of 5G evolution and beyond. By addressing these challenges and exploring emerging technologies, the full potential of network slicing can be realized, ushering in a new era of connectivity, customization, and efficiency across various industries and applications.

VIII. CONCLUSION

The evolution of network slicing within the 5G ecosystem represents a transformative journey that holds immense promise for reshaping the landscape of wireless communication. This comprehensive exploration of network slicing has delved into its technical foundations, challenges, applications, and future directions, highlighting its pivotal role in meeting the diverse and dynamic demands of modern applications and services. As evidenced by the case studies, network slicing has already demonstrated its versatility and effectiveness in addressing a wide array of use cases. From enhancing the quality of multimedia applications to supporting critical services in healthcare, industry, and emergency response, network slicing has proven to be a powerful tool for customization, efficiency, and reliability. Looking ahead, the future directions outlined underscore the potential for continued innovation and advancement. Integrating network slicing with emerging technologies like AI and blockchain, extending its capabilities beyond 5G into future wireless standards, and tailoring slices for specific industry verticals are crucial steps in unlocking its full potential. The emphasis on security and privacy enhancements reflects the growing importance of ensuring the trustworthiness of network slices, particularly in an era of increasing cyber threats and concerns about data privacy. The convergence of network slicing with edge computing and the exploration of sustainable and green networking practices further solidify its relevance in building a technologically advanced yet environmentally conscious communication infrastructure.

In conclusion, network slicing stands as a cornerstone for ushering in a new era of connectivity one that is dynamic, customizable, and responsive to the unique requirements of diverse applications and industries. The ongoing research, collaboration, and standardization efforts will continue to shape the trajectory of network slicing, making it a pivotal component in the continued evolution of wireless communication networks. As we navigate the path toward 6G and beyond, the lessons learned from network slicing in 5G will undoubtedly guide us toward a future where connectivity is not just ubiquitous but also tailored to the specific needs of a digitally interconnected world.

IX. REFERENCES

[1] R. Bolla, R. Bruschi, F. Davoli, and F. Cucchietti, "5G Mobile Networks: A Survey," Int. J. Business Data Commun. Networking, vol. 15, no. 3, pp. 211-233, 2019.

[2] M. A. Aazam and E. Huh, "Fog-supported smart cities: A survey of networking architectures and IoT integration," ACM Transactions on Internet Technology (TOIT), vol. 18, no. 3, p. 34, 2018.

[3] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," IEEE Communications Magazine, vol. 52, no. 5, pp. 86-92, 2014.

[4] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dut.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Cloud Computing Poses Security Challenges And Risks

KADALI ANJANI
23DSC09, M.Sc.(Computational Data Science)
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
anjanikadali286@gmail.com

RAVADA VARSHA
23DSC14,M.Sc.(Computational Data Science
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
Ravadavarsha@gmail.com

PATNALA MEGHANA
23DSC04,M.Sc.(Computational Data Science)
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
meghanapatnala786@gmail.com

ABSTRACT: Cloud Computing Means Storing and Accessing the Data and Programs on Remote Servers That Are Hosted on The Internet Instead of The Computer's Hard Drive or Local Server. Cloud Computing Is Also Referred to As Internet-Based Computing, It Is A Technology Where the Resource Is Provided as A Service Through the Internet to The User. The Data Which Is Stored Can Be Files, Images, Documents, Or Any Other Storable Document. Cloud Computing Has Taken Its Place All Over the IT Industries. It is an On-Demand Internet-Based Computing Service That Provides the Maximum Result with Minimum Resources Cloud Computing Provides A Service That Does Not Require Any Physical Close to The Computer Hardware. Cloud Computing Is A Product of Grid, Distributed, Parallel, And Ubiquitous Computing. This Paper Introduces the Concepts, History Pros, And Cons of Cloud Computing. Now Coming to Iot, It Can Be Any Device Equipment, Or Object Which Connects Us with The Cloud Using the Internet or With Another Device That Is Connected. It Has Sensors, Processing Ability, Software, And Many Technologies Which Can Be Used to Share and Fetch Data or Information with Other Devices and Servers Over the Internet. Nowadays Big Companies Are Using Cloud Services for Storing Their Data Because It Is Easy to Manage Their Data Easily Without Any Additional Costs. Cloud Computing Provides Us the Flexibility to Play with Our Data and Gives Us More Freedom with Storage, Access, And Management. In This Paper, We Will See the Advantages and Disadvantages of Using the Cloud, How Iot Is Useful in Cloud Systems, And How We Can Overcome the Problems Related to The Cloud.

KEYWORDS: Cloud Computing, Internet-Based Computing.

I. INTRODUCTION

Cloud Computing concept has emerged from the distributed software architecture. Cloud computed technology is aimed to provide hosted services over the internet. In recent years, cloud computing in Information Technology has given rise to various new user communities and markets [1]. Cloud computing services are provided from data centers located in different parts of the world. Microsoft SharePoint and Google applications are general examples of cloud computing services. Cloud computing is everywhere. Pick up any tech magazine or visit almost any IT website or blog and you'll be sure to see talk about cloud computing. The only problem is that not everyone agrees on what it is. Ask ten different professionals what cloud computing is, and you'll get ten different answers. And is cloud computing even worth all the hype? Some people don't think so. In fact, in 2008 Oracle CEO Larry Ellison chastised the whole issue of cloud computing, saying that the term was overused and being applied to everything in the computer world. Berkeley RAD Lab defines Cloud Computing as follows: Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing [2]. Cloud computing is a model where services are added on the way to use the services over the Internet which are dynamically scaled. In the past, the cloud was often used to represent part of the Internet with some infrastructure. Nowadays Cloud is used as a metaphor for the services provided over the Internet. The rapid evolution of cloud services, cloud computing now supports a large number of operations in a fraction of seconds compared to traditional systems where the number of transactions was limited. This computational power can be used for anything such as pre- cloud services users still need to connect with their devices to access and work on these virtual devices with massive processing power around world [3]. Cloud Computing is a network-built handling invention where information is provided to customers on demand. Cloud Computing is a registering phase for dissemination of advantages and assets that involve structures, programming, applications, introduction and commerce. Distributed computing is a robotic supply of handling assets [4]. There is a widespread use of cloud computing (CC) in information technology. However, many service owners are still reluctant to fully adopt the CC as relevant security technologies are not as yet matured. Thus, literature shows a need for service providers to invest in CC-associated device security [6]. We have found a few studies that show the proposal of evaluation of cloud computing security. One of these research studies introduces an "attack tree map" (ATM) to analyze security vulnerabilities and threats. Research [7] highlights various facets of CC combined with the trusted computing platform to provide security services such as confidentiality, authentication, and integrity.

II. RELATED WORK

1. Security and risks and challenge of cloud computing

There are several security risks to consider when making the switch to cloud computing. Some of the top security risks of cloud computing include:

1.Limited visibility into network operations
2.Malware
3.Compliance
4.Data Leakage
5.Inadequate due diligence
6.Data breaches
7.Poor application programming interface (API)

Let's take a closer look at these risks.

1. Limited Visibility into Network Operations

When moving workloads and assets to the cloud, organizations forfeit a certain level of visibility into network operations. This is because the responsibility of managing some of the systems and policies shifts to the cloud service provider. Depending on the type of service model being used, the shift of responsibility may vary in scope. As a result, organizations must be able to monitor their network infrastructure without the use of network-based monitoring and logging.

2. Malware

By moving large amounts of sensitive data to an internet-connected cloud environment, organizations are opening themselves up to additional cyber threats. Malware attacks are a common threat to cloud security, with studies showing that nearly 90% of organizations are more likely to experience data breaches as cloud usage increases. As cybercriminals continue to become increasingly savvy with their attack delivery methods, organizations must be aware of the evolving threat landscape.

3. Compliance

Data privacy is becoming a growing concern, and as a result, compliance regulations and industry standards such as GDPR, HIPAA, and PCI DSS are becoming more stringent. One of the keys to ensuring ongoing compliance is by overseeing who can access data and what exactly they can do with that access. Cloud systems typically allow for large-scale user access, so if the proper security measures (i.e. access controls) aren't in place, it can be difficult to monitor access across the network.

4. Data Leakage

Data leakage is a growing concern for organizations, with over 60% citing it as their biggest cloud security concern. As previously mentioned, cloud computing requires organizations to give up some of their control to the CSP. This can mean that the security of some of your organization's critical data may fall into the hands of someone outside of your IT department. If the cloud service provider experiences a breach or attack, your organization will not only lose its data and intellectual property but will also be held responsible for any resulting damages.

5. Inadequate Due Diligence

The move to the cloud should not be taken lightly. Similar to a third-party vendor, when working with a cloud service provider, it's important to conduct thorough due diligence to ensure that your organization has a complete understanding of the scope of work needed to successfully and efficiently move to the cloud. In many cases, organizations are unaware of how much work is involved in a transition and the cloud service provider's security measures are often overlooked.

6. Data Breaches

One of the most impactful security risks the cloud faces is the potential for a data breach. These are a result of poor security measures that allow malicious actors to gain access to sensitive data across cloud servers. One breach could cost an organization millions of dollars, alongside a blow to an organization's reputation and the potential for legal liability.

7. Poor API

If the cloud has poor Application Program Interfaces (API), then servers run the risk of having data unwillingly exposed. When it comes to API, malicious actors will employ several strategies such as brute force attacks and denial-of-service attacks in order to weaken the integrity of
the system.

III. PROPOSED WORK

We propose the following security methods to safeguard the CLOUD COMPUTING from various security attacks.

Algorithm:

1. Begin
2. Identify potential CLOUD COMPUTING Device Security Threats.
3. Focus on the Most Probable Threats That Could Harm Resources.
4. Determine Security Measures to protect Resources.

5. Put in place Measures to Effectively Protect Resources.
6. Asses the Level of Security to Prevent Unauthorized Access.
7. End

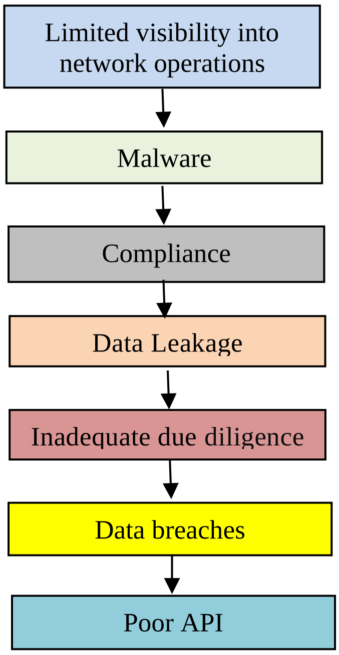


Fig.1. various risks in cloud

Measures to Overcome from Security Risks in Cloud Computing.

1. Security of Data

In terms of security concerns of cloud technology, we don't find answers to some questions. Mysterious threats like website hacking and virus attack are the biggest problems of cloud computing data security. Before utilizing cloud computing technology for a business, entrepreneurs should think about these things. Once you transfer important data of your organization to a third party, you should make sure you have a cloud security and management system. Cybersecurity experts are more aware of cloud security than any other IT professional. According to Crowd Research Partners survey, 9 out of 10 cybersecurity experts are concerned regarding cloud security. Also, they are worried about the violation of confidentiality, data privacy, and data leakage and loss. Vendor Tera data also conducted a cloud analytics survey that reveals that 46% of those reviewed signified more security with no cloud computing challenge.

2. Insufficiency of Resources and Expertise

The inadequacy of resources and expertise is one of the cloud migrations challenges this year. As per the report by Right Scale, almost 75% of the respondent marked it as a challenge while 23% said that it was a serious challenge. Although many IT employees are taking different initiatives to improve their expertise in cloud computing future predictions, employers still find it challenging to find employees with the expertise that they require. According to the Robert Half Technology 2019 Salary Guide, businesses will only prioritize the tech employees with the knowledge and skills of the most recent growth in the cloud, mobile, open-source, big data, security, and other technologies in the upcoming years. Some organizations are also expecting to win over the challenges of shifting to cloud computing by employing more workers with certifications or skills in cloud computing. Industry professionals also suggest providing training of present employees to make them more productive and speedier using the trendiest technology.

3. Complete Governance Over IT Services

IT always doesn't have full control over provisioning, infrastructure delivery, and operation in this cloud-based world. This has raised the complicacy of IT to offer important compliance, governance, data quality, and risk management. To eradicate different uncertainties and difficulties in shifting to the cloud, IT should embrace the conventional control and IT management procedures to incorporate the cloud. Ultimately, basic IT teams' role in the cloud has emerged over the last few years. Alongside the business unites, core IT plays an increasing role in the mediation, preference, and control over cloud services. Moreover, third-party cloud computing or management providers are gradually offering best practices and government support.

4. Cloud Cost Management

The Right Scale report revealed that for a few companies, handling cloud spending has passed security as the biggest cloud computing challenge. As per their anticipations, organizations are ruining nearly 30% of the money they invest in the cloud. Companies make several mistakes that can increase their expenses. Sometimes, IT professionals like developers turn on a cloud instance implied to be utilized for some time and forget to turn it off again. And some companies find themselves hindered by the hidden cloud costing packages that provide numerous discounts that they might not be using. Using cloud spending management challenges, several tech solutions can help organizations. For instance, automation, cloud spending management solutions, serverless services, containers, autoscaling features, and numerous management tools provided by the cloud vendors may help lower the possibility of the issue. Furthermore, some companies have been succeeded by building a core cloud team for handling usage and costs.

5. Dealing with Multi-Cloud Environments

These days, maximum companies are not only working on a single cloud. As per the Flexera 2023 State of the Cloud Report, nearly 87% of the companies are following a multi-cloud strategy and 72% already have their hybrid cloud tactic that is combined with the public and private cloud. Furthermore, organizations are utilizing five distinct public and private clouds.

A long-term prediction on the future of cloud computing technology gives a more difficulty encountered by the teams of IT infrastructure. To win over this challenge, professionals have also suggested the top practices like re-thinking procedures, training staff, tooling, active vendor relationship management, and doing the study.

IV. CONCLUSION

Even through several measures are implemented using security protocols/firewalls which are unable to protect the vulnerabilities of CLOUD COMPUTING devices. Hackers/introduces are continuously making attempt to gain the unauthorized access of CLOUD COMPUTING devices using various attacks. As CLOUD COMPUTING devices usage has increased privacy and security challenges will have an effect on their usage. In Order to protect the security and integrity of CLOUD COMPUTING Devices several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

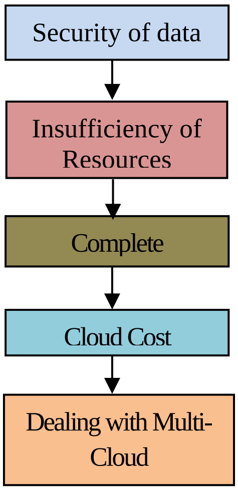


Fig.2.various measures in cloud

V. REFERENCE

[1] Bader Alofi et.al, “A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies”, 14 April 2021, DOI: 10.1109/ACCESS.2021.3073203, Electronic ISSN: 2169-3536

[2] Shyam Patidar et.al, “A Survey Paper on Cloud Computing”, 07-08 January 2012, DOI: 10.1109/ACCT.2012.15, Electronic ISSN: 2327-0659

[3] Jayachander Surbiryala et.al, “Cloud Computing: History and Overview”, 08-10 August 2019, DOI: 10.1109/CloudSummit47114.2019.00007, Electronic ISBN:978-1-7281-3101-6

[4] Neeraj Singla et.al, “A Review Paper on Cloud Computing”,IEEE , 23-24 December 2022 , DOI: 10.1109/CISCT55310.2022.10046572 , Electronic ISBN:978-1-6654-7416-0

[5] Jayachander Surbiryala et.al, “Cloud Computing: History and Overview”, 08-10 August 2019, DOI: 10.1109/CloudSummit47114.2019.00007, Electronic ISBN:978-1-7281-3101-6

[6] Nader F. Mir et.al, “Cloud and Edge Computing”, June 2020, DOI: 10.1109/MCOMSTD.2020.9139038 Electronic ISSN: 2471-2833

[7] Shyam Patidar et.al, “A Survey Paper on Cloud Computing”, 07-08 January 2012, DOI: 10.1109/ACCT.2012.15, Electronic ISSN: 2327-0659

[8] Tharam Dillon et.al, “Cloud Computing: Issues and Challenges”, 20-23 April 2010, DOI: 10.1109/AINA.2010.187, Electronic ISBN:978-1-4244-6696-2.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Speak Assist : An NLP and DSP-Driven Text-to-Speech Synthesizer for Enhanced Accessibility and Efficiency

K.NAGA LALITHA SRI
Student,22MCA51,M.C.A
Department of Computer Science
P.B.Siddhartha College Of Arts & Science
Vijayawada,AP,India
nagalalithakomaravolu96@gmail.com

P.DEVIKA
Student, 22MCA06,M.C.A
Department of Computer Science
P.B.Siddhartha College Of Arts & Science
Vijayawada, AP,India
devikapandrangi2000@gmail.com

M. INDRANI
Student , 22MCA07,M.C.A
Department of computer science
P.B.Siddhartha College Of Arts & Science
Vijayawada , AP,India
mettapalliindrani@gmail.com

ABSTRACT: Introducing Speakassist, A Text-To-Speech Synthesizer Application Designed to Transform Written Text into Spoken Words. This Innovative Tool Employs Natural Language Processing (NLP) And Digital Signal Processing (DSP) Technologies to Analyze and Process the Input Text, Creating A Synthesized Speech Representation. Our User-Friendly Application Simplifies the Process, Allowing Users to Input Text, Hear the Synthesized Speech, And Save It as An MP3 File. Additionally, It Preserves the Audio in The Form of An MP3 File, Enabling Users to Store It for Future Use. Developed with The Aim of Aiding Individuals with Visual Impairment, Speakassist Facilitates Easier Navigation Through Large Volumes of Text, Enhancing Accessibility and Efficiency.

KEYWORDS: Text-To-Speech Synthesis, Natural Language Processing, Digital Signal Processing

I. INTRODUCTION

Text-to-speech synthesis, abbreviated as TTS, refers to the automated process of converting written text into speech that closely resembles a native speaker reading the text. The technology behind a text-to-speech synthesizer (TTS) allows a computer to communicate audibly. In this system, the TTS engine takes textual input, analyzes the content using computer algorithms, pre-processes the text, and employs mathematical models to synthesize speech. Typically, the TTS engine produces sound data in an audio format as the final output. The text-to-speech (TTS) synthesis process comprises two primary phases. The first phase involves text analysis, wherein the input text is converted into a phonetic or another linguistic representation. The second phase is the generation of speech waveforms, where the output is derived from the phonetic and prosodic information obtained in the previous step. These phases are commonly referred to as high and low-level synthesis [1]. Figure 1 below illustrates a simplified version of this procedure. The input text could originate from various sources, such as a word processor, standard ASCII from email, a mobile text message, or scanned text from a newspaper. The character string undergoes pre-processing and analysis, resulting in a phonetic representation, typically a string of phonemes with additional information for accurate intonation, duration, and stress. The low-level synthesizer then utilizes this information from the high-level synthesis to generate speech sounds. The artificial production of speech-like sounds has a rich history, with documented mechanical attempts dating back to the eighteenth century.

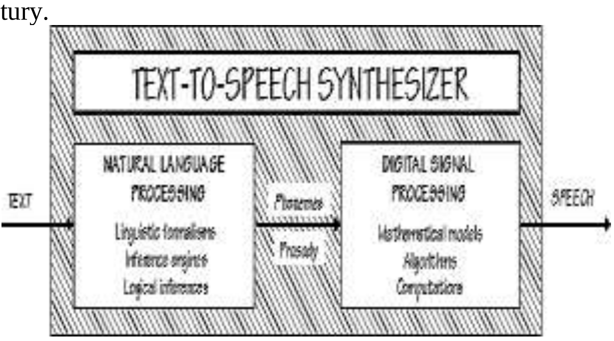


Figure 1: A simple but comprehensive functional diagram of a text-to-speech (TTS) system [2].

II. REVIEW OF LITERAURE

Overview of Speech Synthesis:

Speech synthesis involves the artificial generation of human-like speech [3]. A computer system designed for this purpose is referred to as a speech synthesizer and can be implemented in either software or hardware. Specifically, a text-to-speech (TTS) system is responsible for converting regular language text into speech [4]. Synthesized speech is often produced by combining recorded speech fragments stored in a database. Systems may vary in the size of the stored speech units; for instance, a system storing phones or diphones offers a broad output range but may sacrifice clarity. In contrast, systems storing entire words or sentences are capable of providing high-quality output, especially in specific usage domains. Alternatively, a synthesizer can integrate a model of the vocal tract and other human voice characteristics to generate a fully "synthetic" voice output [5]. The assessment of a speech synthesizer's quality is based on its resemblance to the human voice and its capacity for intelligibility. An effective text-to-speech program enables individuals with visual impairments or reading disabilities to listen to written content on a home computer. A text-to-speech system, also known as an "engine," consists of two main components: a front-end and a back-end [6]. The front-end performs two primary tasks. Initially, it transforms raw text, including symbols like numbers and abbreviations, into the equivalent of fully written-out words. This step is commonly referred to as text normalization, pre-processing, or tokenization. Subsequently, the front-end assigns phonetic transcriptions to each word and segments and annotates the text into prosodic units, such as phrases, clauses, and sentences. The process of assigning phonetic transcriptions to words is known as text-to-phoneme or grapheme-to-phoneme conversion. The combination of phonetic transcriptions and prosody information forms the symbolic linguistic representation produced by the front-end. The back-end, often termed the synthesizer, then transforms the symbolic linguistic representation into audible sound. In some systems, this component includes the calculation of target prosody elements (pitch contour, phoneme durations) [7], which are subsequently applied to the resulting speech output.

Various methods exist for speech synthesis, and the selection depends on the intended task. However, the most commonly utilized approach is Concatenative Synthesis, primarily chosen for its ability to generate synthesized speech that sounds the most natural. Concatenative synthesis operates by concatenating or stringing together segments of recorded speech. Within concatenative synthesis, three primary sub-types can be identified [8]:

Domain-specific Synthesis: Domain-specific Synthesis involves concatenating pre-recorded words and phrases to construct complete utterances, making it suitable for applications where the system's text output is confined to a specific domain, such as transit schedule announcements or weather reports [9]. This technology is straightforward to implement and has a long history of commercial use in devices like talking clocks and calculators. The naturalness of these systems can be quite high, given the limited variety of sentence types, closely matching the prosody and intonation of the original recordings. However, due to the constraints of their databases, these systems are not versatile and can only synthesize combinations of words and phrases for which they have been pre-programmed.

Although domain-specific synthesis handles naturally spoken language well, challenges may arise, particularly in handling variations. For instance, in non-rhotic dialects of English, the pronunciation of the "r" in words like "clear" /ˈklɪə/ typically occurs only when the following word starts with a vowel (e.g., "clear out" realized as /ˌklɪəɾˈʌʊt/) [10]. Similarly, in French, final consonants may no longer be silent if followed by a word starting with a vowel, a phenomenon known as liaison. Simple word-concatenation systems struggle to reproduce such alternations and require additional complexity to be context sensitive.

To implement domain-specific synthesis, the voice of a person speaking the desired words and phrases is recorded. This approach is beneficial when a limited set of phrases and sentences is employed, and the system's text output is confined to a specific domain, such as delivering messages in a train station or providing weather reports or checking a telephone subscriber’s bank balance.

Unit Selection Synthesis: Unit selection synthesis uses large databases of recorded speech. In the process of creating the database, each recorded utterance undergoes segmentation into various components, such as individual phones, diphones, half-phones, syllables, morphemes, words, phrases, and sentences. Typically, this segmentation is carried out using a specially modified speech recognizer set to a "forced alignment" mode, followed by manual correction using visual representations like the waveform and spectrogram [11]. An index of units within the speech database is then generated based on the segmentation and acoustic parameters such as the fundamental frequency (pitch), duration, position in the syllable, and neighbouring phones. During runtime, the desired target utterance is formed by determining the optimal chain of candidate units from the database, a process known as unit selection. This selection process is commonly accomplished using a specially weighted decision tree.

Unit selection synthesis achieves the highest level of naturalness by applying minimal digital signal processing (DSP) to the recorded speech. DSP, when used extensively, can often make recorded speech sound less natural. However, some systems incorporate a small amount of signal processing at the point of concatenation to smooth the waveform. The output from top-performing unit-selection systems is frequently indistinguishable from real human voices, especially in contexts where the text-to-speech (TTS) system. Nevertheless , achieving maximum naturalness typically necessitates very large unit-selection speech databases, with some systems extending into gigabytes of recorded data, representing dozens of hours of speech [12].It’s worth noting that unit selection algorithms may, at times , select segments from a less-than-ideal location, leading to suboptimal synthesis, such as minor words becoming unclear, even when a better choice exists in the database[13].

Diphone Synthesis: Diphone synthesis relies on a compact speech database that includes all the diphones, representing sound-to-sound transitions, found in a language. The quantity of diphones is contingent upon the phonotactics of the language; for instance, Spanish encompasses about 800 diphones, while German has approximately 2500. In diphone synthesis, the speech database contains only one instance of each diphone. During runtime, the desired prosody of a sentence is applied to these minimal units through digital signal processing techniques like linear predictive coding, PSOLA [12], or MBROLA [14]. The quality of the resulting speech in diphone synthesis is generally inferior to that of unit-selection systems but superior to the output of formant synthesizers. Diphone synthesis inherits some of the sonic glitches associated with concatenative synthesis and the somewhat robotic-sounding nature of formant synthesis. Despite these drawbacks and its limited advantages, such as a small size, diphone synthesis is experiencing a decline in commercial applications. Nevertheless, it continues to be utilized in research due to the availability of freely accessible software implementations [15].

III. METHODOLOGY

Structure of a Text-to-speech Synthesizer system
Text-to-speech synthesis involves a series of steps. TTS systems receive a text as input, which they initially analyze and subsequently convert into a phonetic description. In a

subsequent step, they generate the prosody. Using the gathered information, the system can then generate a speech signal.
The structure of the text-to-speech synthesizer can be broken down into major modules:

i. **Natural Language Processing (NLP) Module**
This module generates a phonetic transcription of the input text, along with prosodic information

ii. **Digital Signal Processing (DSP) Module**
This module converts the symbolic information received from NLP into clear and audible speech.

The major operations of the NLP module are as follows:
Text Analysis: Initially, the text undergoes segmentation into tokens. The process of token-to-word conversion involves creating the orthographic form of each token. For instance, the token "Mr" is expanded to its orthographic form "Mister," the token "12" is converted to "twelve," and "1997" is transformed into "nineteen ninety-seven."

Application of Pronunciation Rules: Following the completion of text analysis, pronunciation rules come into play. Direct 1:1 transformation of letters into phonemes is not always feasible due to non-parallel correspondence. In specific contexts, a single letter may correspond to either no phoneme (e.g., "h" in "caught") or multiple phonemes (e.g., "m" in "Maximum"). Furthermore, multiple letters may correspond to a single phoneme (e.g., "ch" in "rich").
There are two approaches for determining pronunciation:

1. In a dictionary-based solution, with morphological components, the emphasis is on storing as many morphemes (words) as possible in a dictionary. Full forms are then generated through the application of inflection, derivation, and composition rules. Alternatively, a comprehensive full-form dictionary is employed, storing all potential word forms. Pronunciation rules come into play for words not found in the dictionary.
2. In a rule-based solution, pronunciation rules are derived from the phonological knowledge present in dictionaries. The dictionary primarily includes words whose pronunciation is entirely exceptional, and for other words, the rules govern their pronunciation.

The two applications differ significantly in the size of their dictionaries. The dictionary-based solution is many times larger than the rules-based solution’s dictionary of exception. However, dictionary-based solutions can be more exact than rule-based solution if they have a large enough phonetic dictionary available.
Prosody Generation: Following the establishment of pronunciation, the next step involves generating prosody. The naturalness of a TTS system is contingent on various prosodic elements, including intonation modeling (phrasing and accentuation), amplitude modeling, and duration modeling. This encompasses the duration of sound, the duration of pauses, determining the length of syllables, and controlling the tempo of the speech [16].

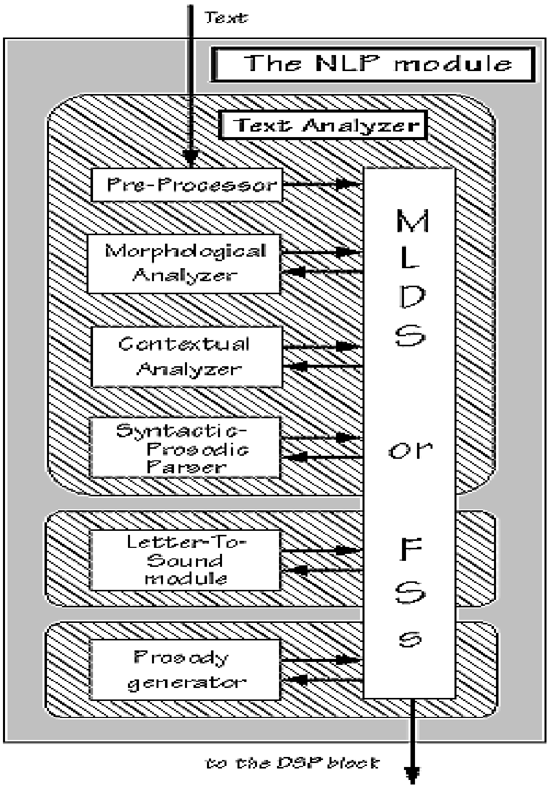


Figure 2: Operations of the natural Language processingmodule of a TTS synthesizer.

The output from the NLP module is forwarded to the DSP module, which is the stage where the synthesis of the speech signal occurs. In concatenative synthesis, the process involves selecting and linking speech segments. For individual sounds, the optimal choice is made from a database, and these selected segments are then concatenated.

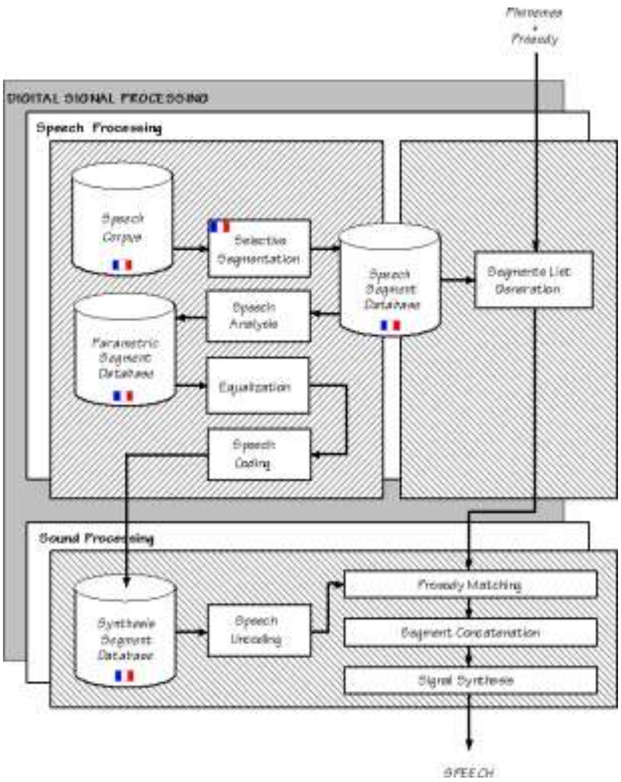


Figure 3: The DSP component of a general concatenation-based synthesizer.

IV. RESULTS AND DISCUSSION

Design & Implementation:

Our software, named TextToSpeech Robot, is a straightforward application that offers text-to-speech functionality. The system was crafted using the Java programming language, chosen for its robustness and platform independence.

The application comprises two primary modules:

1. **Main Application module**: This module incorporates basic GUI components responsible for fundamental operations of the application. These operations include parameter input for conversion, achieved either through file input, direct keyboard input, or browser interaction. The main application module utilizes the open-source APIs SWT and DJNativeSwing.
2. **Main Conversion Engine module:** Integrated into the main module, this module is dedicated to data acceptance and subsequent conversion. The engine implements the freeTTS API to facilitate the text-to-speech conversion process.

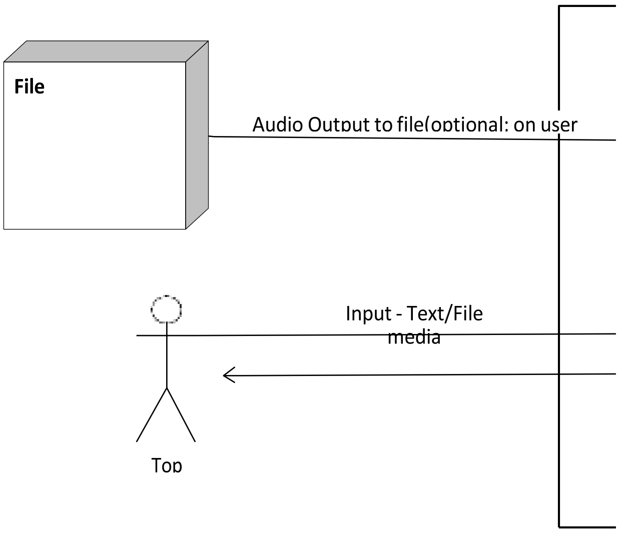
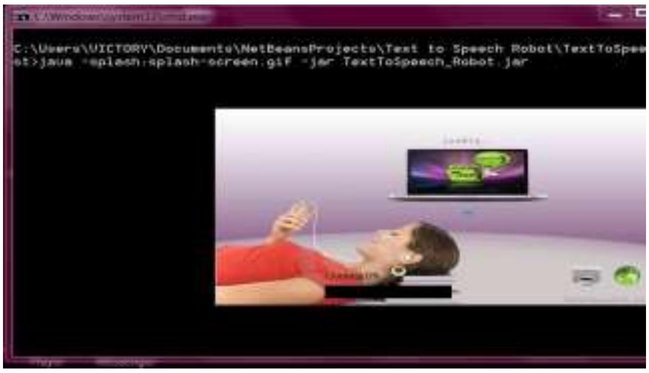


Figure 4: TTS Synthesis System Architecture.

TextToSpeech Robot (TTSR) facilitates the conversion of text to speech through two methods: either by entering the text directly into the provided text field or by copying content from a local document and pasting it into the application's text field. Additionally, the application includes a feature enabling users to browse the World Wide Web (www) within the application. TTSR is equipped to read aloud specific portions of web pages. Users can achieve this by highlighting the desired section and then clicking the "Play" button.

TTSR includes a unique feature that allows users to save their converted text to any location on their local machine in an audio format. This flexibility enables users to copy the audio file to their preferred audio devices.



```
C:\Users\VICTORY\Documents\NetBeansProjects\Text to Speech Robot\TextToSpee
ot>java -splash:splash-screen.gif -jar TextToSpeech_Robot.jar
```

Figure 5: The Loading phase of the application.

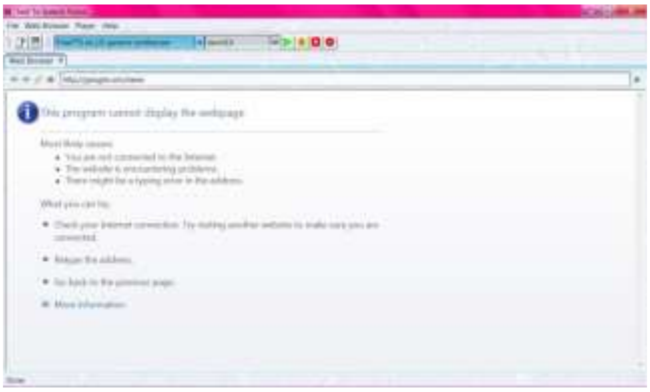
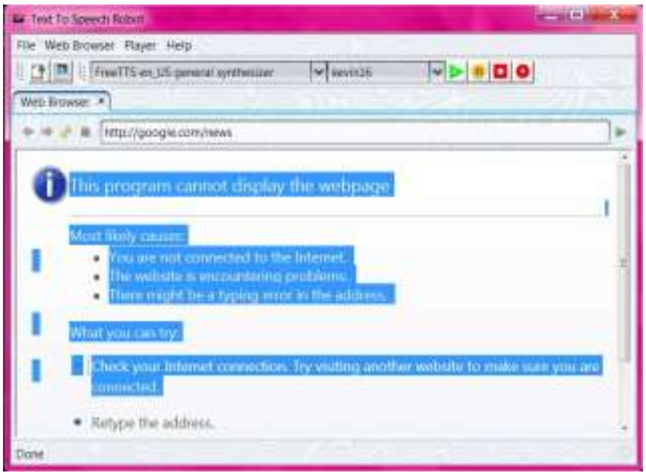


Figure 6: Screenshot of the Text To Speech RobotInterface

Upon loading, the default view of the application is the web browser interface. The web browser indicates a lack of internet connection on the local machine, displaying the message "The page cannot be displayed." In this browser view, any highlighted section within the application can be read aloud by TTSR. Users have the flexibility to select and convert any portion of the web page using the application's highlighting feature.



Text To Speech Robot
File Web Browser Player Help
FreeTTS en_US general synthesizer
kevin16
Web Browser
http://google.com/news

This program cannot display the webpage

Most likely causes:

- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

What you can try:

- Check your Internet connection. Try visiting another website to make sure you are connected.
- Retype the address.

Figure 7: A part of the web page in the application being highlighted waiting for conversion.

The Standard Tool Bar

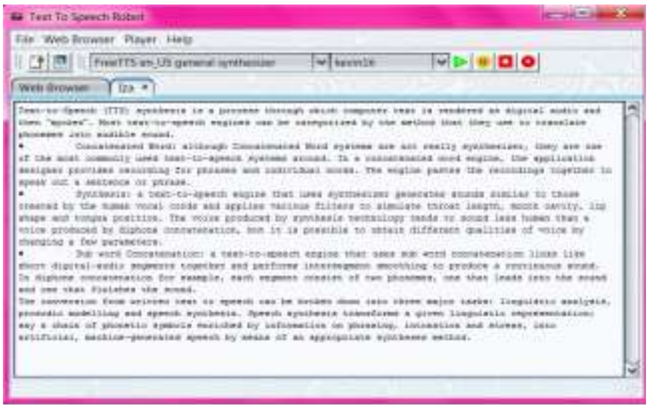
The toolbar includes standard options such as File, Web Browser, Player, and Help.

Within the **File Menu**, users are provided with the option to either open a new browser or open a new text field for importing text documents.

The **Player Menu** offers users the flexibility to play, stop, or pause the speech. Additionally, it includes a functional "Record" button, enabling the export of the audio speech to any location on the local machine.

The text field:

The text field serves as the space for typing or loading all textual content. This field contains the text that will be processed and read by the engine.



Text To Speech Robot
File Web Browser Player Help
FreeTTS en_US general synthesizer
kevin16
Web Browser
tza

Text-to-Speech (TTS) synthesis is a process through which computer text is rendered as digital audio and then "spoken". Most text-to-speech engines can be categorized by the method that they use to translate phonemes into audible sound.

- Concatenated Word: although Concatenated Word systems are not really synthesizers, they are one of the most commonly used text-to-speech systems around. In a concatenated word engine, the application designer provides recordings for phrases and individual words. The engine pastes the recordings together to speak out a sentence or phrase.
- Synthesis: a text-to-speech engine that uses synthesizer generates sounds similar to those created by the human vocal cords and applies various filters to simulate throat length, mouth cavity, lip shape and tongue position. The voice produced by synthesis technology tends to sound less human than a voice produced by diphone concatenation, but it is possible to obtain different qualities of voice by changing a few parameters.
- Sub word Concatenation: a text-to-speech engine that uses sub word concatenation links like short digital-audio segments together and performs intersegment smoothing to produce a continuous sound. In diphone concatenation for example, each segment consists of two phonemes, one that leads into the sound and one that finishes the sound.

The conversion from written text to speech can be broken down into three major tasks: linguistic analysis, prosodic modelling and speech synthesis. Speech synthesis transforms a given linguistic representation, say a chain of phonetic symbols enriched by information on phrasing, intonation and stress, into artificial, machine-generated speech by means of an appropriate synthesis method.

Figure 8: The TTSR Interface when a text document is loaded into it.

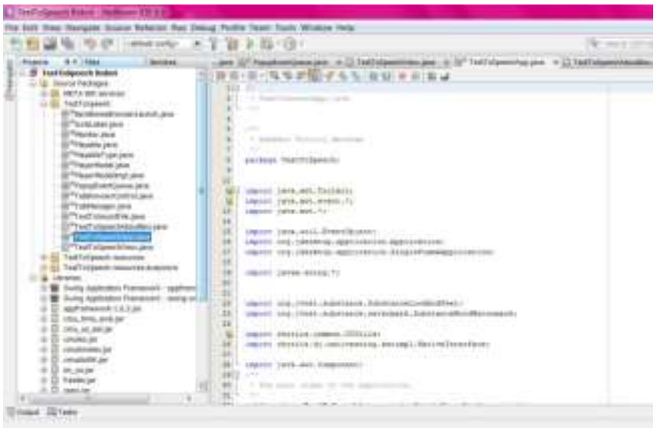


Figure 9: Work in progress of the creation of the application in the NetBeans Environment.

V. CONCLUSION

Text-to-speech synthesis is a rapidly advancing facet of computer technology and is progressively assuming a more significant role in our interactions with systems and interfaces across diverse platforms. We have identified the various operations and processes integral to text-to-speech synthesis. Additionally, we have designed an intuitive graphical user interface, allowing users to input text in the provided field within the application. Our system interfaces with a text-to-speech engine tailored for American English. Looking ahead, we plan to expand our efforts by creating engines for localized Nigerian languages, aiming to enhance the accessibility of text-to-speech technology to a broader range of Nigerians. Similar initiatives have been successful in implementing such systems in native languages like Swahili [18], Konkani [19], the Vietnamese synthesis system [10], and the Telugu language [20]. Another avenue for future work involves implementing a text-to-speech system on various platforms, including telephony systems, ATM machines, video games, and other platforms where text-to-speech technology would enhance functionality and provide added advantages.

VI. REFERENCES

[1] Lemmetty, S., 1999. Review of Speech Syn1thesis Technology. Masters Dissertation, Helsinki University Of Technology.

[2] Dutoit, T., 1993. High quality text-to-speech synthesis of the French language. Doctoral dissertation, Faculte Polytechnique de Mons.

[3] Suendermann, D., Höge, H., and Black, A., 2010. Challenges in Speech Synthesis. Chen, F., Jokinen, K., (eds.), *Speech Technology*, Springer Science + Business Media LLC.

[4] Allen, J., Hunnicutt, M. S., Klatt D., 1987. From Text to Speech: The MITalk system. Cambridge University Press.

[5] Rubin, P., Baer, T., and Mermelstein, P., 1981. An articulatory synthesizer for perceptual research. Journalof the Acoustical Society of America 70: 321–328.

[6] van Santen, J.P.H., Sproat, R. W., Olive, J.P., and Hirschberg, J., 1997. Progress in Speech Synthesis. Springer.

[7] van Santen, J.P.H., 1994. Assignment of segmental duration in text-to-speech synthesis. Computer Speech & Language, Volume 8, Issue 2, Pages 95–128.

[8] Wasala, A., Weerasinghe R. , and Gamage, K., 2006, Sinhala Grapheme-to-Phoneme Conversion and Rules for Schwaepenthesis. Proceedings of the COLING/ACL 2006 Main Conference Poster Sessions, Sydney, Australia, pp. 890-897.

[9] Lamel, L.F., Gauvain, J.L., Prouts, B., Bouhier, C., and Boesch, R., 1993. Generation and Synthesis of Broadcast Messages, Proceedings ESCA-NATO Workshop and Applications of Speech Technology.

[10] van Truc, T., Le Quang, P., van Thuyen, V., Hieu, L.T., Tuan, N.M., and Hung P.D., 2013. Vietnamese Synthesis System, Capstone Project Document, FPTUNIVERSITY.

[11] Black, A.W., 2002. Perfect synthesis for all of the people all of the time. IEEE TTS Workshop.

[12] Kominek, J., and Black, A.W., 2003. CMU ARCTIC databases for speech synthesis. CMU-LTI-03-177. Language Technologies Institute, School of ComputerScience, Carnegie Mellon University.

[13] Zhang, J., 2004. Language Generation and Speech Synthesis in Dialogues for Language Learning. Masters Dissertation, Massachusetts Institute of Technology.

[14] Dutoit, T., Pagel, V., Pierret, N., Bataille, F., van der Vrecken, O., 1996. The MBROLA Project: Towards a set of high quality speech synthesizers of use for non- commercial urposes. ICSLP Proceedings.

[15] Text-to-speech (TTS) Overview. In Voice RSS Website. Retrieved February 21, 2014, from http://www.voicerss.org/tts/

[16] Text-to-speech technology: In Linguatec Language Technology Website. Retrieved February 21, 2014, from http://www.linguatec.net/products/tts/information/technology

[17] Dutoit, T., 1997. High-Quality Text-to-Speech Synthesis:An Overview. Journal Of Electrical And Electronics Engineering Australia 17, 25-36.

[18] Ngugi, K., Okelo-Odongo, W., and Wagacha, P. W., 2005. Swahili Text-To-Speech System. African Journal of Science and Technology (AJST) Science and Engineering Series Vol. 6, No. 1, pp. 80 – 89.

[19] Mohanan, S., Salkar, S., Naik, G., Dessai, N.B., andNaik, S., 2012. Text To Speech Synthesizer for Konkani Language. International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, ISBN 978-1-4675-2248-9.

[20] Swathi, G., Mai, C. K., and Babu, B. R., 2013. Speech Synthesis System for Telugu Language. International Journal of Computer Applications (0975 – 8887), Volume 81 – No5.

A Study on Internet of Things Concept Across Different Applications

M.VECHAN PRABHU KUMAR
Student , 22DSC19, M.Sc.(Data Science)
Department of Computer Science
P.B.Siddhartha College Of Arts & Science
Vijayawada,AP,India
prabhukumarvechan@gmail.com

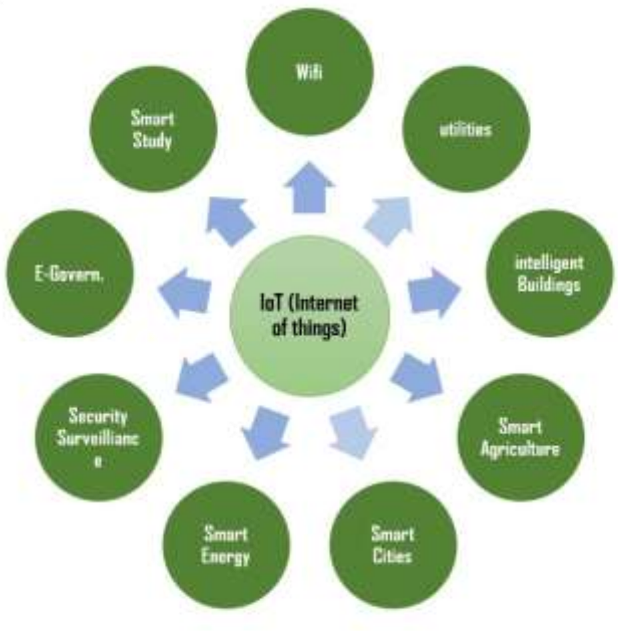
A.KAVITHA
Lecture
Department of Computer Science
P.B.Siddhartha College Of Arts & Science
Vijayawada,AP,India
kavitha@pbsiddhartha.ac.in

P.JAGADISH
Student, 22DSC25, M.Sc.(Data Science)
Department of Computer Science
P.B.Siddhartha College Of Arts & Science
Vijayawada,AP,India
Penugondajagadish123@gmail.com

ABSTRACT: The Internet of Things (IOT) Describes A Kind of Network Which Interconnects Various Devices with The Help of Internet. IOT Assists to Transmit Data with Among Devices, Tracing and Monitoring Devices and Other Things. IOT Make Objects 'Smart' By Allowing Them to Transmit Data and Automating of Tasks, Without Lack of Any Physical Interference. A Health Tracking Wearable Device Is an Example of Simple Effortless IOT In Our Life. A Smart City with Sensors Covering All Its Regions Using Diverse Tangible Gadgets and Objects All Over the Community and Connected with The Help of Internet. This Word IOT Was First Suggested by Kevin Ashton in 1999. The Subsequent Segment Represent Fundamental Of IOT. It Hands Out Several Covering Pre-Owned in IOT and Varied Fundamental Denominations Connected. It is Primarily Enlargement of Helping-Hand Using Internet. When the Household Devices are Connected with the Help of Internet, This Can Help to Automate Homes, Offices or Other Units Using IOT. IOT is Being Used During COVID-19 Pandemic for Contact Tracing.

I. INTRODUCTION

The Internet of Things (IoT) is an emerging paradigm that enables the communication between electronic devices and sensors through the internet in order to facilitate our lives. IoT use smart devices and internet to provide innovative solutions to various challenges and issues related to various business, governmental and public/private industries across the world [1]. IoT is progressively becoming an important aspect of our life that can be sensed everywhere around us. In whole, IoT is an innovation that puts together extensive variety of smart systems, frameworks and intelligent devices and sensors (Fig.1). Moreover, it takes advantage of quantum and nanotechnology in terms of storage, sensing and processing speed which were not conceivable beforehand. Extensive research studies have been done and available in terms of scientific articles, press reports both on internet and in the form of printed materials to illustrate the potential effectiveness and applicability of IoT transformations. It could be utilized as a preparatory work before making novel innovative business plans while considering the security, assurance and interoperability.

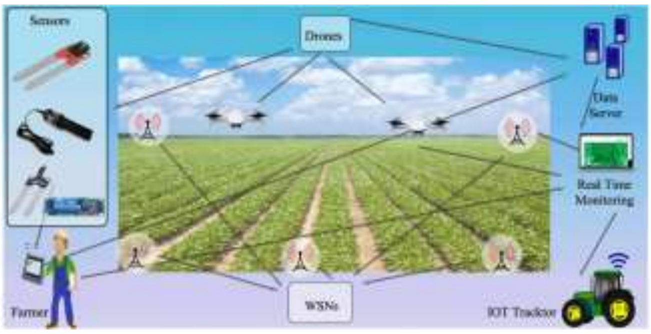


II. SMART CITY

Smart city is one of the trendy application areas of IoT that incorporates smart homes as well. Smart home consists of IoT enabled home appliances, air-conditioning/heating system, television, audio/video streaming devices, and security systems which are communicating with each other in order to provide best comfort, security and reduced energy consumption. All this communication takes place through IoT based central control unit using Internet. The concept of smart city gained popularity in the last decade and attracted a lot of research activities. The smart home business economy is about to cross the 100 billion dollars by 2022. Smart home does not only provide the in-house comfort but also benefits the house owner in cost cutting in several aspects i.e. low energy consumption will results in comparatively lower electricity bill. Besides smart homes, another category that comes within smart city is smart vehicles. Modern cars are equipped with intelligent devices and sensors that control most of the components from the headlights of the car to the engine. The IoT is committed towards developing a new smart car system that incorporates wireless communication between car-to-car and car-to-driver to ensure predictive maintenance with comfortable and safe driving experience

III. AGRICULTURE

The world's growing population is estimated to reach approximate 10 billion by 2050. Agriculture plays an important role in our lives. In order to feed such a massive population, we need to advance the current agriculture approaches. Therefore, there is a need to combine agriculture with technology so that the production can be improved in an efficient way. Greenhouse technology is one of the possible approaches in this direction. It provides a way to control the environmental parameters in order to improve the production. However, manual control of this technology is less effective, need manual efforts and cost, and results in energy loss and less production. With the advancement of IoT, smart devices and sensors makes it easier to control the climate inside the chamber and monitor the process which results in energy saving and improved production (Fig. 9). Automatization of industries is another advantage of IoT. IoT has been providing game changing solutions for factory digitalization, inventory management, quality control, logistics and supply chain optimization and management.



IV. INDUSTRIAL AUTOMATION

Industrial automation's main aim is to reduce the necessity of people in manufacturing processes. This allows production to speed up, increase in safety, and better utilize their resources and industrial analytics in manufacturing. Achieving this goal is accomplished by fully mapping out the industrial process and understanding sub-process relationships so machines can be assigned to work and automate certain process tasks.

Machine automation technology can be set to work as fixed applications, programmable applications, or flexible/adaptable applications. Each of these types of machine automation has certain advantages and disadvantages. Recent advancements in machine automation are due to a better understanding of machine automation and the adoption of new machine capabilities such as feedback controllers, robotics, networking, digital computers, and interconnectivity. Fixed automated machines for example, only work to carry out repetitive and mundane tasks but newly-interconnected, programmable machines can enable manufacturers to offload many process decisions to high-speed controllers, oftentimes operating completely without human intervention.

i. Security Challenge 1: Weak or non-existent authentication

Major challenge facing IoT is weak or non-existent authentication. Many IoT devices are designed with minimal security, making them vulnerable to attacks.

Solution

>Implementing strong authentication methods, such as two-factor authentication, can help ensure that only authorized users have access to the device.

ii. Security Challenge 2: Insufficient network security

IoT devices often connect to the internet using unsecured networks, making them vulnerable to attacks. For example, an attacker could intercept communications between an IoT device and the internet, potentially gaining access to sensitive data.

Additionally, unsecured networks can also be used to launch attacks on other devices on the network.

Solution

>Implementing secure network protocols, such as VPN and HTTPS, can help ensure that data is transmitted securely. Virtual Private Networks (VPNs) can be used to encrypt communications between IoT devices and the internet, making it more difficult for attackers to intercept data.

iii. Security Challenge 3: Limited physical security

Limited physical security is a significant challenge facing IoT devices as they are often small and easy to conceal, making them vulnerable to physical attacks. A physical attack on an IoT device can include tampering, theft, or destruction of the device. This can result in unauthorized access to sensitive information, system downtime, and loss of data.

Solution

>Implementing physical security measures, such as locks and cameras, can help ensure that devices are protected against physical attacks. This can include using tamper-proof enclosures, security locks, and surveillance cameras to monitor the location of the devices.

iv. Security Challenge 4: Inadequate data protection

Inadequate data protection is a significant security challenge facing IoT devices as they generate and collect a large amount of data, making it vulnerable to attacks. This data can include personal information, financial information, and other sensitive information.

If this data is not properly protected, it can fall into the wrong hands and be used for malicious purposes.

Solution

>Implementing access controls can also help ensure that only authorized users have access to the data. This can include using role-based access controls, multi-factor authentication, and other security measures to ensure that only authorized users can access the data.

>Regularly reviewing the physical security of devices and updating the software to the latest version can also help ensure that devices are protected against physical attacks. This includes conducting regular physical security audits, monitoring the device's location, and ensuring that all devices are updated with the latest security patches.

v. Security Challenge 5: Difficulty in detecting and responding to threats

IoT devices, such as smart thermostats, security cameras, and smart appliances, often operate in the background, constantly collecting and transmitting data. Because these devices are connected to the internet and often have minimal user interaction, it can be difficult to detect and respond to security threats.

For example, a hacker may be able to gain access to a device without the user's knowledge and use it to launch a cyber attack.

Solution

>Implement security monitoring and incident response processes. This can include regular monitoring of device activity, as well as implementing tools and techniques to detect unusual or suspicious behavior.

For example, security software can be installed on the device to monitor network traffic and alert administrators to any potential threats.

vi. Security Challenge 6: Lack of visibility and control

IoT devices are designed to operate in the background, often without the user's knowledge or interaction. This can make it difficult to understand their behavior and control their actions.

For example, an IoT device such as a smart camera may be sending data to a cloud service without the user's knowledge. This lack of visibility into the device's behavior can make it difficult to detect and prevent malicious activity.

Solution

>Developing tools to monitor and control IoT devices can help ensure that they are operating as intended by providing visibility into their behavior. This can include monitoring network traffic, identifying and blocking suspicious activity, and tracking device activity over time.

vii. Security Challenge 7: Limited regulatory oversight

The limited regulatory oversight of IoT (Internet of Things) devices can be a major security concern, as it makes it difficult to ensure that these devices are secure. To address this issue, several solutions have been proposed, including

Solution

>Certifying IoT devices and platforms: Certifying IoT devices and platforms can also help ensure that they meet certain security standards. This can include certifications for specific security features, such as encryption and authentication, as well as certifications for compliance with specific security standards, such as ISO 27001.

viii. Security Challenge 8: Inability to update or patch devices

Many IoT devices are difficult or impossible to update or patch, making them vulnerable to attacks. This means that once a vulnerability is discovered, it cannot be fixed, making the device vulnerable to attacks.

Furthermore, some devices are no longer supported by their manufacturers, making it impossible to receive any security updates or patches. This lack of updateability and patch ability makes it difficult to protect these devices from known vulnerabilities and exploits, leaving them open to cyberattacks.

Solution

>Using a secure gateway is another important step in ensuring the security of IoT devices. A secure gateway acts as a central point of control for all devices on the network, and can be used to monitor and control the communication between devices, ensuring that it is secure.

This can include encryption and authentication to prevent unauthorized access to the network.

V. CONCLUSION

In conclusion, the Internet of Things (IoT) has brought about many benefits, but it has also introduced a host of security challenges. These security challenges for IoT include device vulnerabilities, data privacy concerns, and network insecurity. To address these challenges, you can consult an IoT app development company who will implement robust security measures such as device authentication, encryption, and regular software updates. Additionally, IoT devices should be designed with security in mind from the outset, and companies should have a clear and transparent data privacy policy in place. By addressing these security challenges head-on, an IoT app development company with its reliable iot app development services can ensure the safety and security of their devices and the data they collect and transmit.

VI. REFERENCES:

[1] Sfar AR, Zied C, Challal Y. A systematic and cognitive vision for IoT security: a case study of military live simulation and security challenges. In: Proc. 2017 international conference on smart, monitored and controlled

cities (SM2C), Sfax, Tunisia, 17–19 Feb. 2017. https://doi.org/10.1109/sm2c.2017.8071828.

[2] Gatsis K, Pappas GJ. Wireless control for the IoT: power spectrum and security challenges. In: Proc. 2017 IEEE/ACM second international conference on internet-of-things design and implementation (IoTDI), Pittsburg, PA, USA, 18–21 April 2017. INSPEC Accession Number: 16964293.

[3] Zhou J, Cap Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: challenges. IEEE Commun Mag. 2017;55(1):26–33. https://doi.org/10.1109/MCOM.2017.1600363CM.

[4] Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw. 2018;4(1):118–37.

[5] Minoli D, Sohraby K, Kouns J. IoT security (IoTSec) considerations, requirements, and architectures. In: Proc. 14th IEEE annual consumer communications & networking conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017. https://doi.org/10.1109/ccnc.2017.7983271.

[6] Gaona-Garcia P, Montenegro-Marin CE, Prieto JD, Nieto YV. Analysis of security mechanisms based on clusters IoT environments. Int J Interact Multimed Artif Intell. 2017;4(3):55–60.

[7] Behrendt F. Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities. Sustainability. 2019;11(3):763.

[8] IoT application areas. https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/. Accessed 05 Apr 2019.

[9] Zanella A, Bui N, Castellani A, Vangelista L, Zorgi M. Internet of things for smart cities. IEEE IoT-J. 2014;1(1):22–32.

Mobile Security Unleashed : Safeguarding Your Digital World

I.SIVAJI
Student, 23MCA40, M.C.A
Department of Computer Scince
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
23MCA40@pbsiddhartha.ac.in

N.SAI
Student, 23MCA22, M.C.A
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
23MCA22@pbsiddhartha.ac.in

A.N.SIVA KUMAR
Student, 23MCA38, M.C.A
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
23MCA38@pbsiddhartha.ac.in

ABSTRACT: Communicating mobile security threats and best practices has become a central objective due to the ongoing discovery of new vulnerabilities of mobile devices. To cope with this overarching issue, the goal of this paper is to identify and analyze existing threats and best practices in the domain of mobile security. To this extent, we conducted a literature review based on a set of keywords. The obtained results concern recognizable threats and established best practices in the domain of mobile security. Afterwards, this outcome was put forward for consideration by mobile application users (n = 167) via a survey instrument. To this end, the results show high awareness of the threats and their countermeasures in the domain of mobile applications. While recognizing the risks associated with physical and social factors, the majority of respondents declared the use of built-in methods to mitigate the negative impact of malicious software and social-engineering scams.[1][2][3] The study results contribute to the theory on mobile security through the identification and exploration of a variety of issues, regarding both threats and best practices. Besides this, this bulk of up-to-date knowledge has practical value which reflects in its applicability at both the individual and enterprise level. Moreover, at this point, we argue that understanding the factors affecting users' intentions and motivations to accept and use particular technologies is crucial to leverage the security of mobile applications. Therefore, future work will cover identifying and modeling users' perceptions of the security and usability of mobile applications.

KEYWORDS: Mobile, Security, Vulnerability, Attacks, Penetration Test.

I. INTRODUCTION

Cyber breaches have dominated headlines as attacks targeting more and more users will have grown dramatically. Mobile technology seems to be an easy target for cybercriminals who seek financial gain by stealing credit card data or personal information that can be re-sold or used for extortion. Criminal networks have reaped immense profits and are able to invest into investigating and developing more sophisticated methods and skills, which are then available through online forums for anyone to purchase. Meanwhile, there is no dependable and effective defense mechanism for mobile technology to fend off such attacks. The lack of knowledge or training to face today's security challenges remains an issue with the users of mobile devices. This study revolves around "malware" and its effects on mobile devices. Malware (malicious software) is defined as any software used to damage computer operations, penetrate sensitive information, gain access to personal computer systems, or display unsolicited advertising. These programs are designed to infiltrate and damage computers without the users' consent. Computer Viruses, Worms, Trojan Horses, and Spyware, are some examples. Viruses can cause destruction on a computer's hard drive by deleting files or directory information.

Fig 1. Mobile Security

II. RELATED WORK

Mobile security faces various types of attacks that threaten the confidentiality, integrity, and availability of data. Here are some common types of attacks on mobile security:

1. **Data Leakage:**

Mobile apps are often the cause of unintentional data leakage. For example, "riskware" apps pose a real problem for mobile users who grant them broad permissions, but don't always check security. These are typically free apps found in official app stores that perform as advertised, but also send personal and potentially corporate data to a remote server, where it is mined by advertisers, and sometimes, by cybercriminals.[4]

2. Unsecured Wi-Fi:
No one wants to burn through their cellular data when wireless hot spots are available but free Wi-Fi Mobiles are usually unsecured. According to V3, in fact, three British politicians who agreed to be part of a free wireless security experiment were easily hacked by technology experts. Their social media, PayPal and even their VoIP conversations were compromised. To be safe, use free Wi-Fi sparingly on your mobile device. And never use it to access confidential or personal services, like banking or credit card information.[5]

3. Mobile Spoofing:
Mobile spoofing is when hackers set up fake access points connections that look like Wi-Fi Mobiles, but are actually traps in high-traffic public locations such as coffee shops, libraries and airports. Cybercriminals give the access points common names like “Free Airport Wi-Fi” or “Coffeehouse” to encourage users to connect.[6]

4. Phishing Attacks:
Because mobile devices are always powered-on, they are the front lines of most phishing attack. According to CSO, mobile users are more vulnerable because they are often monitor their email in real-time, opening and reading emails when they are received. Mobile device users are also more susceptible because email apps display less information to accommodate the smaller screen sizes. For example, even when opened, an email may only display the sender’s name unless you expand the header information bar. Never click on unfamiliar email links. And if the matter isn’t urgent, then let the response or action items wait until you’re at your computer.[7]

5. Spyware:
Although many mobile users worry about malware sending data streams back to cybercriminals, there’s a key threat closer to home: Spyware. In many cases, it’s not malware from unknown attackers that users should be worried about, but rather spyware installed by spouses, co-workers or employers to keep track of their whereabouts and activity. Also known as stalker ware, many of these apps are designed to be loaded on the target’s device without their consent or knowledge. A comprehensive antivirus and malware detection suite should use specialized scanning techniques for this type of program, which requires slightly different handling than does other malware owing to how it gets onto your device and its purpose.[8]

6. Broken Cryptography:
According to Infosec Institute training materials, broken cryptography can happen when app developers use weak encryption algorithms, or fail to properly implement strong encryption. In the first case, developers may use familiar encryption algorithms despite their known vulnerabilities to speed up the app development process. As a result, any motivated attacker can exploit the vulnerabilities to crack passwords and gain access. In the second example, developers use highly secure algorithms, but leave other “back doors” open that limit their effectiveness. For example, it may not be possible for hackers to crack the passwords, but if developers leave flaws in the code that allow attackers to modify high-level app functions such as sending or receiving text messages, they may not need passwords to cause problems. Here, the onus is on developers and organizations to enforce encryption standards before apps are deployed.

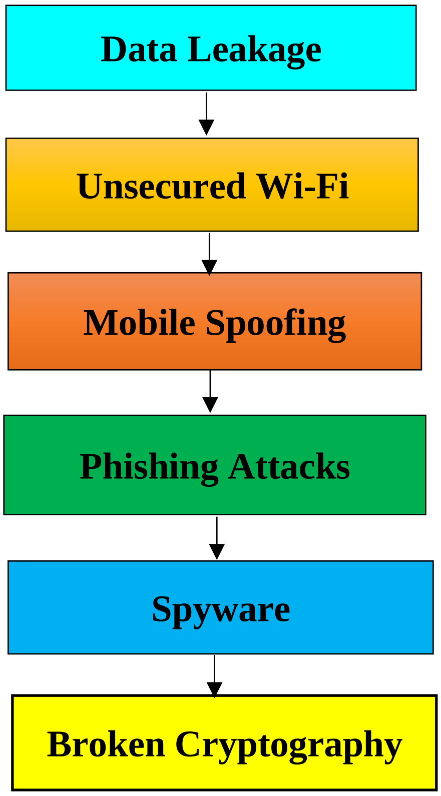


Fig.2 Threats on Mobile security

III. PROPOSED WORK

Certainly! Mobile Security is the critical aspect of ensuring the confidentiality, integrity, and availability of data in a Mobile. Here are some proposed work areas for Mobile security:

1. Use strong passwords/biometrics:
Strong passwords and biometric features, such as fingerprint authenticators, make unauthorized access nearly impossible. Your passwords should be eight or more characters long and contain alphanumeric characters. The complexities of your passwords in other apps might tempt you to store them like a browser does using the 'remember me’ feature. Device users and administrators should avoid this feature since it only increases the chances of your password getting spoofed. Alternatively, if you lose your device, another person might gain full access to it. With that comes access to accounts where you have valuable data such as banking and payments

systems. Furthermore, don't forget to change your password from time to time [9].

2. Install an Antivirus application:
The files you download and the apps you install on your mobile device might contain malicious code. Once launched, this code could send your data to criminals, making you unsecured and robbing you of your privacy. To avoid that, installing a reputable antivirus application will improve your security.[10]

3. Utilize a VPN:
If you're unsure about the security status of the Mobile you're connected to, using a VPN (Virtual Private Mobile) client is mandatory. A VPN will enable you to connect to a Mobile securely. At the same time, the VPN will shield your browsing activity on public wifi from prying eyes. It is also useful when accessing less secure sites. VPN services are relatively inexpensive and are invaluable for protecting your website traffic and private information. Non-HTTPS sites are visible to anyone who knows how to use Mobileing and vulnerability tools. These sites are prone to MITM (man-in-the-middle) attacks, which pave the way to eavesdropping and password sniffing. You need to have a new mindset when it comes to fighting cybercrime.

4. Install an Antivirus application:
The files you download and the apps you install on your mobile device might contain malicious code. Once launched, this code could send your data to criminals, making you unsecured and robbing you of your privacy. To avoid that, installing a reputable antivirus application will improve your security. Some offer more functionalities, such as erasing your data if you lose your mobile device, tracking and blocking unknown callers who might be a threat, and telling you which applications are unsafe. In addition, they offer to clear your browsing history and delete cookies. Cookies are small software tokens that store your login information that might be leaked if someone malicious gets to them.

5. Update to the latest software:
Your mobile device firmware might also be vulnerable to security threats. New loopholes might be exploited, leaving your device open to threats. To avoid that, always update your firmware/device. Major mobile device firmware companies, such as Google's Android and Apple's iOS roll out new updates from time to time. Most of those updates act as a security patch to known vulnerabilities on your device. Set up updates to be manual or automatic, and don't delay these installations for long.

6. Ensure public or free wifi is protected:
Everybody loves free wifi, especially if your data plan is limited. But cheap can turn expensive in a very devastating manner because most free wifi points are not encrypted. These open Mobiles allow cybercriminals to eavesdrop on the Mobile traffic and quickly get your passwords, usernames, and other sensitive information. For a skilled cybercriminal, it could only take moments to for your data to land in the wrong hands.

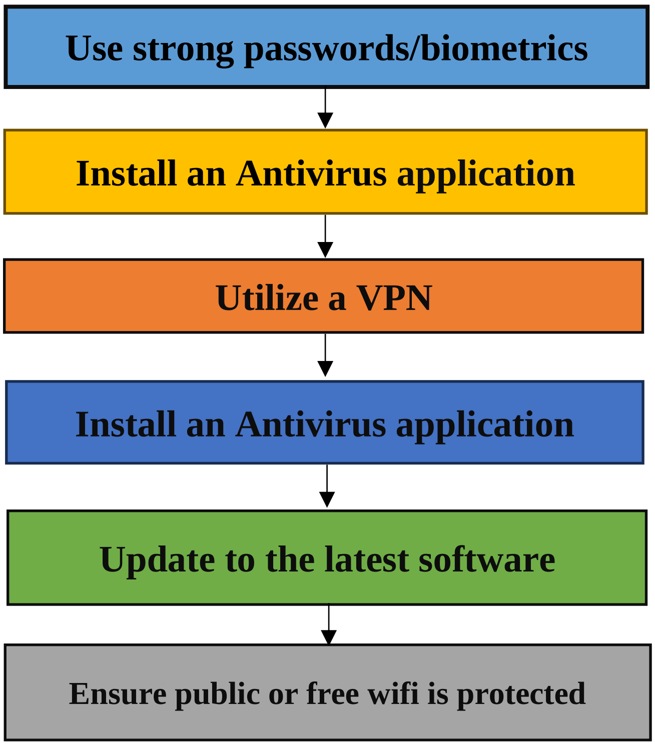

Use strong passwords/biometrics
Install an Antivirus application
Utilize a VPN
Install an Antivirus application
Update to the latest software
Ensure public or free wifi is protected

Fig.3 Safety Measures for Mobile Security

Algorithm:
1. Begin
2. Identify Mobile security problems.
3. Focus on the Most Probable Mobile Security Risks.
4. Determine various Security Measures to Protect our Mobile and Data.
5. Implement Measures Protect the Mobile Data.
6. Assess the Level of Security implemented in Mobile to Prevent Unauthorized Access.
7. End

IV. RESULT & ANALYSIS

S.No.	Types of Attacks possible on Mobile security	Percentage of Vulnerability
1	Data Leakage	15
2	Unsecured Wi-Fi	14
3	Mobile Spoofing	23
4	Phishing Attacks	16
5	Spyware	18
6	Broken Cryptography	14
Vulnerability before the implementation of Proposed Security Measures		100

Table 1. Types of possible Attacks on Mobile security

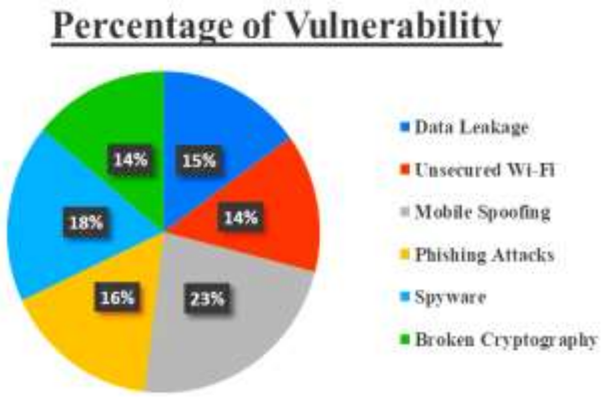


Fig. 4. Vulnerability before the application of Proposed Security Measures

S.No.	Types of Attacks possible on Mobile security	Percentage of Vulnerability
1	Data Leakage	5.2
2	Unsecured Wi-Fi	2.4
3	Mobile Spoofing	4.7
4	Phishing Attacks	6.1
5	Spyware	6.4
6	Broken Cryptography	5.2
Vulnerability after the implementation of Proposed Security Measures		30

Table 2. Types of possible Attacks on Mobile security

Fig.5 Vulnerability after the application of Proposed Security Measures

V. CONCLUSION & FUTURE WORK

In conclusion, mobile security is an indispensable aspect of our interconnected digital lives, given the ubiquity of smartphones and tablets. As these devices store and access sensitive personal and corporate information, safeguarding them is imperative. The multifaceted nature of mobile security involves protecting against a variety of threats, including malware, phishing attacks, and unauthorized access. Implementing robust security measures such as secure authentication, encryption, and regular software updates is essential to fortify the resilience of mobile devices against potential vulnerabilities. Additionally, user education plays a pivotal role in fostering a security-conscious mindset, encouraging individuals to adopt responsible practices and be vigilant against emerging threats. The dynamic nature of the mobile landscape requires continuous adaptation and innovation in security strategies to stay ahead of malicious actors. Ultimately, a proactive and comprehensive approach to mobile security is crucial for ensuring the privacy, integrity, and reliability of the vast array of information processed and stored on our mobile devices.

VI. REFERENCES

[1] Aidan Fuller et. al, "Digital Twin: Enabling Technologies, Challenges and Open Research", May 2020, IEEE, EISSN: 2169-3536, Page(s): 108952-108971, DOI: 10.1109/ACCESS.2020.2998358

[2] A. Bilberg and A. A. Malik, ‘‘Digital twin driven human–robot collaborative assembly,’’ CIRP Ann., vol. 68, no. 1, pp. 499–502, 2019.

[3] C. Mandolla, A. M. Petruzzelli, G. Percoco, and A. Urbinati, ‘‘Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry,’’ Comput. Ind., vol. 109, pp. 134–152, Aug. 2019.

[4] N. Mohammadi and J. E. Taylor, ‘‘Smart city digital twins,’’ in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Nov. 2017, pp. 1–5.

[5] M. Grieves, ‘‘Digital twin: Manufacturing excellence through virtual factory replication,’’ NASA, Washington, DC, USA, White Paper 1, 2014.

[6] XiaoxiaZheng et.al, “Computer Mobile security and measures”, September 2011, IEEE DOI: 10.1109/EMEIT.2011.6023622.

[7] ZHANG Ke, “Research on Internet Data Security and Privacy Protection”, 2021, Journal of Physics: Conference Series, IOP Publishing, doi:10.1088/1742-6596/2005/1/012004

[8] A. K. Maurya et.al, “Ransomware: Evolution, Target and Safety Measures”, JCSE International Journal of Computer Sciences and Engineering, Volume 6, Issue 1, Jan 2018, E-ISSN: 2347-2693, https://www.ijcseonline.org/

[9] R. Ritchey,“Using model checking to analyze Mobile vulnerabilities”, Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000, DOI: 10.1109/SECPRI.2000.848453.

[10] Octavia Georgiana Dorobantuet. al, “Security threats in IoT”,IEEE, January 2021, DOI: 10.1109/ISETC50328.2020.9301127

Adaptive Knowledge Dynamics : Exploring Techniques and Applications in Machine Unlearning

SHAIK BIBI FATHIMA
Student, 22DSC29, M.Sc(CDS)
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, AP, India
bibifathima2002@gmail.com

G SAMRAT KRISHNA
Lecturer (Asst. Professor)
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, AP, India
gsamratkrishna@pbsiddhartha.ac.in

YOGA SRI RAJYA LAKSHMI CHAKKA
Student, 22DSC27, M.Sc(CDS)
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, AP, India
ysrlakshmi2022@gmail.com

ABSTRACT: In the Realm of Machine Learning, The Primary Emphasis Typically Revolves Around Training Models to Discern Patterns and Formulate Predictions or Decisions Based on Available Data. The Concept of "Unlearning" Pertains to The Process of Adjusting or Revising A Pre-Trained Model to Intentionally Discard or Ignore Specific Patterns or Information. This Adjustment Becomes Relevant in Scenarios Where the Model Has Acquired Insights from Data That Have Become Outdated or Inaccurately Reflective of The Current Circumstances. In Today's Digital Landscape, Computer Systems Store Vast Amounts of Personal Data, Enabling Breakthroughs in Artificial Intelligence (AI), Particularly Machine Learning. However, The Abundance of Data Poses Risks to User Privacy and Can Erode the Trust Between Humans And AI. To Address These Concerns, Recent Regulations, Commonly Known As "The Right to Be Forgotten", Mandate the Removal of Private User Information from Computer Systems and Machine Learning Models. While Erasing Data from Back-End Databases Is Relatively Straightforward, It Is Insufficient in The Context of AI Since Machine Learning Models Often Retain Memories of The Old Data. Additionally, Recent Adversarial Attacks on Trained Models Have Demonstrated the Ability to Identify Whether Instances or Attributes Belonged to The Training Data. This Necessitates A New Approach Called Machine Unlearning to Make Machine Learning Models Forget Specific Data. However, Existing Works on Machine Unlearning Have Yet to Fully Solve the Problem Due to The Lack of Standardized Frameworks and Resources.

In the Era Of AI, Where the Significance of Privacy and Data Protection Is on The Rise, The Concept of Machine Unlearning Becomes A Pivotal Instrument for Safeguarding User Privacy and Building Trust. This All-Encompassing Survey Offers Insights into The Foundational Principles, Methodologies, And Practical Applications of Machine Unlearning. By Addressing Gaps In Current Research and Spotlighting Untapped Potentials, We Aim to Stimulate Further Exploration and Innovation in This Field. We Anticipate That This Survey Will Prove to Be A Valuable Resource for Researchers and Practitioners Seeking to Enhance Their Understanding and Implementation of Machine Unlearning in The Realm of Privacy Preservation.

KEYWORDS: Machine Unlearning, Privacy Preservation, Artificial Intelligence (AI).

I. INTRODUCTION

In the rapidly evolving environment of machine learning, the exploration of innovative methodologies and applications is essential to address emerging challenges. This paper delves into the realm of "Adaptive Knowledge Dynamics," focusing on the intricate interplay of techniques and applications within the domain of machine unlearning. As the field of machine learning continues to advance, the need to adapt models to changing circumstances, correct biases, and safeguard privacy becomes increasingly paramount. "Adaptive Knowledge Dynamics" involves a diverse approach to understanding, modifying, and optimizing machine learning models through the lens of unlearning.

This exploration involves scrutinizing the fundamental principles that support adaptive knowledge dynamics, uncovering various techniques employed in the process of machine unlearning, and investigating real-world applications where these dynamics prove pivotal. By connecting theoretical concepts with practical applications, this paper aims to provide a comprehensive overview, nurturing a deeper understanding of the adaptive knowledge dynamics involved in the unlearning process. As we commence on this journey, the goal is to inspire further research, innovation, and practical implementations in the field of machine unlearning. By illuminating the techniques and applications encapsulated within adaptive knowledge dynamics, we seek to contribute to the ongoing discussion, paving the way for advancements that ensure the resilience, adaptability, and ethical considerations of machine learning models in an ever-evolving technological setting.

II. RELATED WORKS

There are various reasons why users might want to delete their data from a system. We can categorize these reasons into four main groups: security, privacy, usability, and fidelity. Each of these reasons is discussed in more detail below.

1. Security:

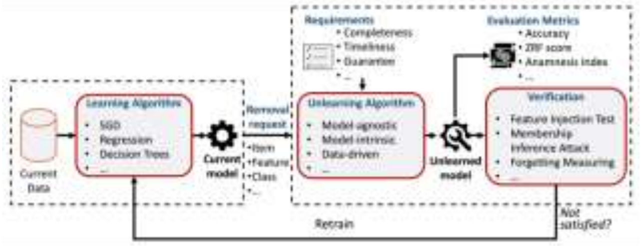
Deep learning models have recently revealed vulnerabilities to external attacks, particularly adversarial attacks. In an adversarial attack, the attacker generates adversarial data that closely resembles the original data to the point where human perception cannot distinguish between the real and fake data. This adversarial data is purposely crafted to manipulate deep learning models, causing them to generate inaccurate predictions, often leading to significant consequences. For instance, in healthcare, an erroneous prediction could result in misdiagnosis, inappropriate treatment, or even loss of life. Therefore, it is imperative to detect and remove adversarial data to ensure the security of the model. Once an attack is identified, the model must be capable of deleting the adversarial data through a machine unlearning mechanism.

2. **Privacy:** Numerous privacy-preserving regulations have recently been implemented, encompassing the right to be forgotten, such as the General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act. These regulations grant users the right to request the deletion of their data and related information in order to safeguard their privacy. Such legislation has emerged in response to instances of privacy breaches. For example, cloud systems can inadvertently expose user data due to multiple copies stored by various entities, backup policies, and replication strategies. In another scenario, machine learning techniques used in genetic data processing have been found to unintentionally disclose patients' genetic markers. Hence, it is unsurprising that users seek to remove their data to mitigate the risks of data leaks.

3. **Usability:** People have diverse preferences when it comes to online applications and services, particularly recommender systems. An application's recommendations can be inconvenient if it fails to completely remove incorrect data (e.g., noise, malicious data, out-of-distribution data) associated with a user. For instance, if someone unintentionally searches for an illegal product on their laptop and continues to receive recommendations for that product on their phone, even after clearing their web browser history, it leads to undesired usability (Y. Cao and Yang, 2015). Such persistent data retention not only results in inaccurate predictions but also reduces user satisfaction and engagement.

4. **Fidelity:** Biased machine learning models can prompt requests for unlearning. Despite recent advancements, machine learning models are still susceptible to bias, resulting in outputs that unfairly discriminate against specific groups of people. For instance, COMPAS, a software employed by courts to determine parole cases, demonstrates a higher tendency to assign elevated risk scores to African-American offenders compared to Caucasians, even when ethnicity information is not included as input. Similar instances of bias have been observed in beauty contests judged by AI, which exhibited prejudice against participants with darker skin tones, as well as facial recognition AI systems that inaccurately recognized Asian facial features. The origin of these biases can often be traced back to the data itself. For instance, AI systems trained on public datasets that predominantly feature individuals of white ethnicity, such as ImageNet, are more prone to making errors when processing images of individuals with black ethnicity. Similarly, in an application screening system, the machine learning model might unintentionally acquire inappropriate features, such as gender or race information, during the learning process. Consequently, there is a necessity to unlearn such data, which involves discarding the associated features and affected data items.

The unlearning framework in presents the typical workflow of a machine learning model in the presence of a data removal request. In general, a model is trained on some data and is then used for inference. Upon a removal request, the data-to-be-forgotten is unlearned from the model. The unlearned model is then verified against privacy criteria, and, if these criteria are not met, the model is retrained, i.e., if the model still leaks some information about the forgotten data. There are two main components to this process: the learning component (left) and the unlearning component (right). The learning component involves the current data, a learning algorithm, and the current model. In the beginning, the initial model is trained from the whole dataset using the learning algorithm. The unlearning component involves an unlearning algorithm, the unlearned model, optimization requirements, evaluation metrics, and a verification mechanism. Upon a data removal request, the current model will be processed by an unlearning algorithm to forget the corresponding information of that data inside the model. The unlearning algorithm might take several requirements into account such as completeness, timeliness, and privacy guarantees. The outcome is an unlearned model, which will be evaluated against different performance metrics. However, to provide a certificate for the unlearned model, a verification (or audit) is needed to prove that the model actually forgot the requested data and that there are no information leaks. This audit might include a feature injection test, a membership inference attack, forgetting measurements, etc.

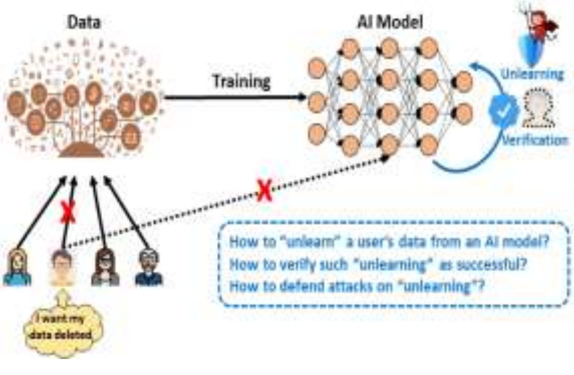


A Typical Machine Unlearning Process

If the unlearned model passes the verification, it becomes the new model for downstream tasks (e.g., inference, prediction, classification, recommendation). If the model does not pass verification, the remaining data, i.e., the original data excluding the data to be forgotten, needs to be used to retrain the model. Either way, the unlearning component will be called repeatedly upon a new removal request.

III. OBJECTIVE

This paper's goal is to investigate and confirm the efficiency of machine unlearning within adaptive knowledge dynamics. Key goals include formulating a conceptual framework, examining methodologies, evaluating practical applications, establishing performance metrics, ensuring adaptability to dynamic changes, addressing ethical considerations, promoting user-centric integration, and contributing to the dissemination of knowledge and collaborative efforts. The overarching aim is to advance the comprehension and practical implementation of machine unlearning for the refinement of dynamic knowledge and the enhancement of system resilience.


Data
Training
AI Model
Unlearning
Verification
How to "unlearn" a user's data from an AI model?
How to verify such "unlearning" as successful?
How to defend attacks on "unlearning"?
I want my data deleted

IV. EXISTING SYSTEM

Completeness (Consistency): A good unlearning algorithm should be complete, i.e. the unlearned model and the retrained model make the same predictions about any possible data sample. One way to measure this consistency is to compute the percentage of the same prediction results on a test data. This requirement can be designed as an optimization objective in an unlearning definition by formulating the difference between the output space of the two models. Many works on adversarial attacks can help with this formulation.

Timeliness: In general, retraining can fully solve any unlearning problem. However, retraining is time-consuming, especially when the distribution of the data to be forgotten is unknown. As a result, there needs to be a trade-off between completeness and timeliness. Unlearning techniques that do not use retraining might be inherently not complete, i.e., they may lead to some privacy leaks, even though some provable guarantees are provided for special cases. To measure timeliness, we can measure the speed up of unlearning over retraining after an unlearning request is invoked.

Accuracy: An unlearned model should be able to predict test samples correctly. Or at least its accuracy should be comparable to the retrained model. However, as retraining is computationally costly, retrained models are not always available for comparison. To address this issue, the accuracy of the unlearned model is often measured on a new test set, or it is compared with that of the original model before unlearning.

Light-weight: To prepare for unlearning process, many techniques need to store model checkpoints, historical model updates, training data, and other temporary data. A good unlearning algorithm should be light-weight and scale with big data. Any other computational overhead beside unlearning time and storage cost should be reduced as well.

Provable guarantees: With the exception of retraining, any unlearning process might be inherently approximate. It is practical for an unlearning method to provide a provable guarantee on the unlearned model. To this end, many works have designed unlearning techniques with bounded approximations on retraining. Nonetheless, these approaches are founded on the premise that models with comparable parameters will have comparable accuracy.

Model-agnostic: An unlearning process should be generic for different learning algorithms and machine learning models, especially with provable guarantees as well. However, as machine learning models are different and have different learning algorithms as well, designing a model-agnostic unlearning framework could be challenging.

Verifiability: Beyond unlearning requests, another demand by users is to verify that the unlearned model now protects their privacy. To this end, a good unlearning framework should provide end-users with a verification mechanism. For example, backdoor attacks can be used to verify unlearning by injecting backdoor samples into the training data. If the backdoor can be detected in the original model while not detected in the unlearned model, then verification is considered to be a success. However, such verification might be too intrusive for a trustworthy machine learning system and the verification might still introduce false positive due to the inherent uncertainty in backdoor detection.

Stream Removal: Handling data streams where a huge amount of data arrives online requires some mechanisms to retain or ignore certain data while maintaining limited storage. In the context of machine unlearning, however, handling data streams is more about dealing with a stream of removal requests.

V. PROPOSED SYSTEM

1. **Item Removal:** Requests to remove certain items/samples from the training data are the most common requests in machine unlearning.

2. **Feature Removal:** In many scenarios, privacy leaks might not only originate from a single data item but also in a group of data with the similar features or labels. For example, a poisoned spam filter might misclassify malicious addresses that are present in thousands of emails. Thus, unlearning suspicious emails might not enough. Similarly, in an application screening system, inappropriate features, such as the gender or race of applicants, might need to be unlearned for thousands of affected applications.

3. **Class Removal:** There are many scenarios where the forgetting data belongs to single or multiple classes from a trained model. For example, in face recognition applications, each class is a person's face so there could potentially be thousands or millions of classes. However, when a user opts out of the system, their face information must be removed without using a sample of their face. Similar to feature removal, class removal is more challenging than item removal because retraining solutions can incur many unlearning passes. Even though each pass might only come at a small computational cost due to data partitioning, the expense mounts up. However, partitioning data by class itself does not help the model's training in the first place, as learning the differences between classes is the core of many learning algorithms. Although some of the above techniques for feature removal can be applied to class removal, it is not always the case as class information might be implicit in many scenarios.

4. **Task Removal:** In general, unlearning a task is uniquely challenging as continual learning might depend on the order of the learned tasks. Therefore, removing a task might create a catastrophic unlearning effect, where the overall performance of multiple tasks is degraded in a domino-effect. Mitigating this problem requires the model to be aware of that the task may potentially be removed in future

5. **Stream Removal:** Handling data streams where a huge amount of data arrives online requires some mechanisms to retain or ignore certain data while maintaining limited storage. In the context of machine unlearning, however, handling data streams is more about dealing with a stream of removal requests.

VI. MACHINE UNLEARNING DEFINITION

While the application of machine unlearning can originate from security, usability, fidelity, and privacy reasons, it is often formulated as a privacy preserving problem where users can ask for the removal of their data from computer systems and machine learning models. The forgetting request can be motivated by security and usability reasons as well. For example, the models can be attacked by adversarial data and produce wrong outputs. Once these types of attacks are detected, the corresponding adversarial data has to be removed as well without harming the model's predictive performance. When fulfilling a removal request, the computer system needs to remove all user's data and 'forget' any influence on the models that were trained on those data. As removing data from a database is considered trivial.

VII. RESULTS

1. **Methodological Advancements:**
   Identification and evaluation of novel methodologies in machine unlearning, demonstrating their effectiveness in dynamically adapting to changing information landscapes.
2. **Conceptual Framework Refinement:**
   Enhancement and refinement of the conceptual framework for adaptive knowledge dynamics, providing a clearer understanding of the role and impact of machine unlearning in knowledge evolution.
3. **Practical Applications:**
   Successful identification and validation of practical applications across diverse domains, showcasing the versatility of machine unlearning in improving model accuracy and adaptability.
4. **Performance Metrics Validation:**
   Development and validation of standardized performance metrics and benchmarks, enabling a comprehensive assessment of the efficiency and effectiveness of various machine unlearning techniques.
5. **Dynamic Adaptability Confirmation:**
   Confirmation of the capability of machine unlearning to dynamically adapt to evolving data landscapes, ensuring sustained relevance and resilience of models over time.
6. **Ethical Considerations Framework:**
   Establishment of an ethical consideration's framework, addressing potential biases and promoting responsible AI practices in the implementation of machine unlearning techniques.
7. **User-centric Integration Insights:**
   Insights into user perceptions and acceptance of machine unlearning, highlighting the importance of user-centric design for practical usability and adoption.
8. **Knowledge Dissemination Impact:**
   Successful dissemination of research findings through academic publications and presentations, contributing to the wider knowledge base and fostering collaboration among researchers, practitioners, and industry experts.

VIII. CONCLUSION

In conclusion, this research on Adaptive Knowledge Dynamics, focusing on machine unlearning techniques and applications, establishes a solid foundation for dynamic knowledge refinement. The study highlights the efficacy of diverse methodologies, demonstrating the versatility of machine unlearning across various domains. Standardized metrics facilitate a comprehensive assessment, emphasizing the advantages of adaptive knowledge dynamics. Ethical considerations and user-centric design underscore responsible implementation. As findings are disseminated, collaborative efforts are expected to propel the integration of machine unlearning into practical applications, marking a significant advancement in the understanding and utilization of these techniques.

IX. REFERENCES

[1] Abadi, Martin, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. "Deep Learning with Differential Privacy." In *SIGSAC*, 308–18.

[2] Aldaghri, Nasser, Hessam Mahdavifar, et al. 2021. "Coded Machine Unlearning." *IEEE Access* 9: 88137–50.

[3] Berahas, Albert S, Jorge Nocedal, et al. 2016. "A Multi-Batch l-BFGS Method for Machine Learning." *NIPS* 29.

[4] Cao, Yinzhi, Alexander Fangxiao Yu, Andrew Aday, Eric Stahl, Jon Merwine, and Junfeng Yang. 2018. "Efficient Repair of Polluted Machine Learning Systems via Causal Unlearning." In *ASIACCS*, 735–47.

[5] Chen, Min, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert, and Yang Zhang. 2021b. "When Machine Unlearning Jeopardizes Privacy." In *SIGSAC*, 896–911.

[6] Halimi, Anisa, Swanand Kadhe, Ambrish Rawat, and Nathalie Baracaldo. 2022. "Federated Unlearning: How to Efficiently Erase a Client in FL?" *arXiv Preprint arXiv:2207.05521*.

[7] Pearce, Tim, Felix Leibfried, and Alexandra Brintrup. 2020. "Uncertainty in Neural Networks: Approximately Bayesian Ensembling." In *AISTATS*, 234–44.

[8] Peste, Alexandra, Dan Alistarh, and Christoph H Lampert. 2021. "SSSE: Efficiently Erasing Samples from Trained Machine Learning Models." In *NeurIPS 2021 Workshop Privacy in Machine Learning*.

[9] Ramaswamy, Vikram V, Sunnie SY Kim, and Olga Russakovsky. 2021. "Fair Attribute Classification Through Latent Space de-Biasing." In *CVPR*, 9301–10.

[10] Sekhari, Ayush, Jayadev Acharya, Gautam Kamath, and Ananda Theertha Suresh. 2021. "Remember What You Want to Forget: Algorithms for Machine Unlearning." *NIPS* 34: 18075–86.

House Price Prediction Using Machine Learning

GUNDA YASASWINI
22DSC22, M.Sc. (Computational Data Science)
Department of Computer Science
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India

ONTERU SUSMITHANJALI
22DSC06, M.Sc. (Computational Data Science)
Department of Computer Science
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India

SRIJA GEDELA
22DSC09, M.Sc. (Computational Data Science)
Department of Computer Science
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India

ABSTRACT: This Paper Introduces a Real Estate Price Prediction System that Uses Machine Learning Algorithms. The System is Intended to Forecast the Price of a Home Grounded on its Various Features Such as Location, Square Footage, Number of Bedrooms and Bathrooms, And Other Related Factors. The System Uses A Variety of Machine Learning Algorithms, Including Linear Regression, Decision Tree Regression, Random Forest Regression, And Artificial Neural Networks to Make Accurate Predictions. Algorithms Are Trained on A Large Dataset of House Prices and Their Associated Characteristics to Learn the Relationships Between These Factors and The Corresponding Prices. The System Is Measured Against Various Performance Metrics, To Measure Its Accuracy and Effectiveness. The Results Show That the System Can Predict House Prices with Great Accuracy, Making It A Valuable Tool for Real Estate Agents, Home Buyers and Sellers. The Implementation of This System Could Lead to Better Informed and More Efficient Decisions in The Housing Market.

KEYWORDS: Random Forest Regressor, Machine Learning, House Price Prediction

I. INTRODUCTION

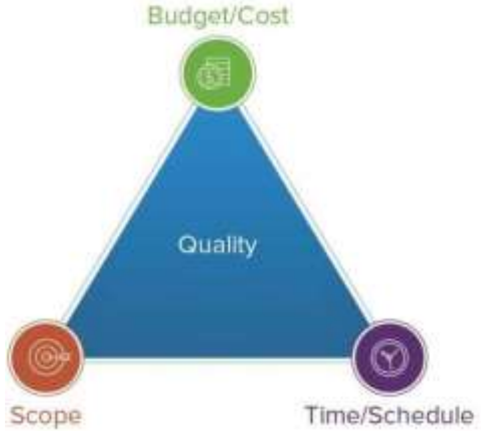
Machine learning has been used for many years to offer image recognition, spam detection, natural speech comprehension, product recommendations and medical diagnoses. Today, machine learning algorithms can help us to enhance cyber security, ensure public safety, and improve medical outcomes. In this project we used a machine learning concept, for example, if we're going to sell a house, we need to know what price tag to put on it. Here the machine learning algorithm can give us an accurate estimation or prediction. Predicting housing prices has always been a challenge for many machine learning engineers. Several researchers have tried to come with a model to accurately predict housing prices with high accuracy and least error. Our goal for this project was to use regression models and classification techniques in order to predict the sale price of a house. These models are created using various features such as square feet of the house, number of bedrooms, year of construction, property type etc. Some of the researchers have used techniques like clustering for grouping same houses together and then estimating the price. In this project we tested a regression models like Simple Linear Regression, Ridge Regression, Lasso Regression, Random Forest Regression, Support Vector Regression, Decision Tree Regression and will choose the best fit among the calculation.

II. PURPOSE

The purpose of this project is to create a machine learning-based system for predicting house prices. This involves utilizing various regression algorithms to analyze a housing dataset and selecting models that achieve the highest accuracy scores. The goal is to assess the effectiveness of machine learning models in estimating house prices on different samples of the dataset. By developing a user-friendly house price prediction system, the aim is to streamline the process and reduce the need for manual intervention. This system would be valuable for both developers and customers. For developers, it assists in determining the optimal selling price for a house, while for customers, it provides valuable information for deciding the right time to purchase a house. Ultimately, the project seeks to leverage machine learning to enhance the efficiency and accuracy of house price predictions, benefiting both sellers and buyers in the real estate market.

III. CONSTRAINTS

We here define the constraint using the triple constraint of project management:



Triple Constraints of Project Management:

1. **Cost:**
   a. The project involves minimal hardware requirements, resulting in low costs.
   b. No significant expenses are incurred due to the absence of hardware elements.
   c. Costs for requirements are kept very low.
   d. Machine learning algorithms require high processing power, met by systems with ample RAM.
   e. Installation of Anaconda, Python libraries (Numpy, Pandas, Seaborn), and Tableau for data science and visualization.
2. **Time:**
   a. Development time depends on project complexity and the number of modules.
   b. Based on current specifications, project deployment is estimated to take approximately 3-4 months.
3. **Scope:**
   a. House Prediction dataset imported from Kaggle in CSV format.
   b. Analysis using Pandas, Numpy, and scikit-learn for machine learning models.
   c. Tableau utilized for data visualization.
   d. Identification of key factors influencing house price changes.
   e. Dataset divided into training and testing sets.
   f. Training machine learning models with the training set.
   g. Performance evaluation using the testing set, calculating accuracy scores and generating confusion matrices.
   h. Root Mean Square Error (RMSE) calculated for all models.
   i. Selection of the model with the highest accuracy and the lowest RMSE for predicting house prices.
   j. Project outcome: Accurate house price predictions beneficial for both customers and developers.

IV. OVERALL SYSTEM DESCRIPTION

i. EXISTING SYSTEM:

In the existing system there are so many solutions for house's sales price prediction problem for one of the Kaggle competitions, in which they combine standard machine learning algorithms with their original ideas like residual regression, logit transform and neural network machine. But during data analysis the results show that the house price variation prediction results is not accurate enough. Sometimes the Standard deviation of the results is very high because of small dataset size.

ii. PROPOSED SYSTEM:

The proposed system effectively addresses existing issues by significantly improving prediction accuracy. It categorizes factors influencing house prices into three main groups: physical condition, concept, and location. Physical condition encompasses observable features like house size, number of bedrooms, kitchen and garage availability, garden presence, building age, etc. The concept refers to developer-offered ideas that attract buyers, such as a minimalist or environmentally friendly home. Location, a crucial factor, shapes house prices based on prevailing land prices and determines access to public facilities and recreational amenities. By optimizing these factors, our system produces more accurate predictions, offering a comprehensive approach to house price estimation.

V. METHODOLOGY

In our project, the House Prediction dataset is imported from Kaggle in Comma Separated Values (csv) format. The dataset is analyzed with the help of pandas, numpy and scikit-learn. Tableau is used as a data visualization tool. After drawing insights from the dataset with the help of Tableau, we identify the important factors i.e. factors majorly affecting the change in prices. The factors adding insignificant values to the overall result are omitted. The dataset is divided into two parts - training set and testing set. The various machine learning models are trained with the help of the training set. The testing set is then used to check the performance of all the machine learning models. Accuracy score is calculated. Root Mean Square Error of all the models is calculated. In the final step the model with the highest accuracy score and the least RMSE (Root Mean Square Error) value is used for predicting house prices.

1. Simple Linear Regression:

In simple linear regression, we predict the scores of a dependent variable (Y') based on the scores of a single independent variable (X). The regression line is represented by the formula: [Y' = bX + A]

Where:

a. (Y') is the predicted score (dependent variable).
b. (X) is the independent variable.
c. (b) is the slope of the line.
d. (A) is the Y-intercept.

In simple linear regression, when there's only one predictor variable (\(X \)), it is referred to as a simple linear regression. The formula simplifies to a straightforward equation for predicting scores based on the linear relationship between the variables.

2. Ridge Regression:

$$\sum_{i=1}^{M}(y_i-\hat{y}_i)^2=\sum_{i=1}^{M}\left(y_i-\sum_{j=0}^{p}w_j\times x_{ij}\right)^2+\lambda\sum_{j=0}^{p}w_j^2$$

Ridge regression is a technique used to modify the loss or errors in a regression model by adding a penalty equivalent to the square of the magnitude of the coefficients. This penalty is introduced to reduce complexity and the overall cost function. The formula for ridge regression is given by:
[text {Ridge} R = text{loss} + lambda ||w||^2]
Here:

a. (lambda) is a constant.
b. (||w||^2) represents the sum of squared coefficients: (w_1^2 + w_2^2 + w_3^2 + ldots), where (w) is a vector of coefficients.

Ridge regression imposes restrictions on the coefficients ((w)), and the penalty term ((lambda)) regularizes these coefficients. If the coefficients become too large, the regularization term penalizes them. Consequently, ridge regression constrains the coefficients, reducing model complexity and addressing issues such as multicollinearity. It proves beneficial in situations where the optimization process needs to be tempered to avoid overfitting and improve the stability of the model.

3. Lasso Linear Regression :

$$\sum_{i=1}^{M}(y_i-\hat{y}_i)^2=\sum_{i=1}^{M}\left(y_i-\sum_{j=0}^{p}w_j\times x_{ij}\right)^2+\lambda\sum_{j=0}^{p}|w_j|$$

Lasso regression, which stands for Least Absolute Shrinkage and Selection Operator, modifies the cost function by adding a penalty term equivalent to the absolute value of the magnitude of the coefficients. The cost function for Lasso regression can be expressed as:
[text {Lasso} = text{loss} + lambda ||w||]
In simpler terms:

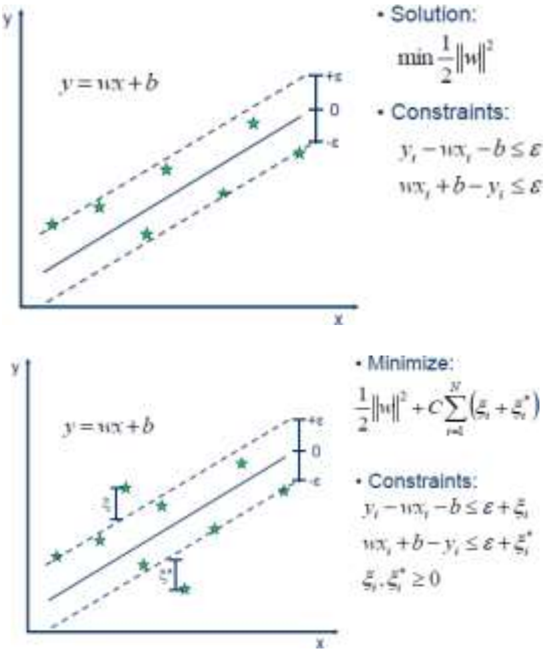
a. (lambda) is a constant.
b. (||w||) represents the sum of the absolute values of coefficients:

(|w_1| + |w_2| + |w_3| + ldots), where (w) is a vector of coefficients.

Lasso regression imposes constraints on the coefficients similar to Ridge regression. The key difference lies in the regularization term, where instead of squaring the coefficients, the absolute values are considered. This type of regularization has the potential to drive some coefficients to exactly zero. Thus, Lasso regression not only aids in minimizing loss/errors in models but also serves as a tool for feature selection. Features with zero coefficients are essentially disregarded in generating the model's outputs, contributing to a simpler and potentially more interpretable model.

4. Support Vector Regression:

SVM, a supervised learning algorithm widely used for classification, is specifically designed for linearly separable data. It employs a "hyperplane" to classify two classes, aiming to create the largest margin in a high-dimensional space for separating the given data into distinct classes.


y
$y = wx + b$
$+\varepsilon$
0
$-\varepsilon$
x
• Solution:
$\min \frac{1}{2}\|w\|^2$
• Constraints:
$y_i - wx_i - b \le \varepsilon$
$wx_i + b - y_i \le \varepsilon$
y
$y = wx + b$
$+\varepsilon$
0
$-\varepsilon$
ξ
ξ^*
x
• Minimize:
$\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{N}(\xi_i + \xi_i^*)$
• Constraints:
$y_i - wx_i - b \le \varepsilon + \xi_i$
$wx_i + b - y_i \le \varepsilon + \xi_i^*$
$\xi_i, \xi_i^* \ge 0$

In simpler terms:

a. **Linear Separability**: SVM works best when the data can be separated by a straight line.
b. **Hyperplane:** The hyperplane is the decision boundary that separates the data into classes.
c. **Margin:** SVM seeks to maximize the margin, representing the distance between the closest data points of the two classes. This ensures a robust separation.

For non-linear data, SVM utilizes kernel functions to map the data into a higher- dimensional space, making it easier to find a hyperplane. The ultimate goal is to find the hyperplane that maximizes the margin, providing a clear distinction between classes and enhancing the model's accuracy in classification tasks.

5. Decision Tree Regression :

Decision tree is a tree shaped figure which is used to determine a course of action. Each branch of the tree represents a possible decision, transpire or reaction. This algorithm makes a classification decision for a test sample with the help of tree like structure. The nodes in the tree are attribute names of the given data. Branches are attribute values and leaf nodes are the class labels.

The advantages of using this algorithm in house price prediction are:

a. It is simple to understand, interpret and visualize.
b. Little effort required for data preparation.
c. It can handle both numerical and categorical data.

6. Random Forest Regression:

Random forest regression develops lots of decision tree based on random selection of variables. It provides the class of dependent variable based on many trees.

a. Random selection of data:

original data= subset 1+subset 2+subset 3+....This subset each can have different size of the observation, there can be some overlapping or cannot.

b. Random selection of variables

If we have variables x1, x2 ...xn independent variables, which can be used for developing decision tree. We divide this variable into different sets like, variable set 1- x1, x3, ... variable set 2- x3, x4...As the trees are based on random selection of data as well as variables, these are random tree. Many such random trees lead to a random forest. When we have many trees, we get a forest, similarly when we have many decision trees it is a random forest. There are two major belief that helps us to use this tree:

i. Most of the trees can provide correct prediction of class for most part of the data.
ii. The tree is making mistakes at different places

VI. REGRESSION RESULTS

Regression	Accuracy Score
Linear Regression	88.82
Lasso	78.56
Ridge	88.83
Random Forest Regression	89.56
SVR (Gaussian kernel)	11.138
Decision Tree Regression	79.56

Prediction and Real Value of a test case with different Regression methods:

Regression	Real Value	Predicted Value
Linear Regression	11.767	11.622
Lasso	11.767	11.566
Ridge	11.767	11.621
Random Forest Regression	11.767	11.767
SVR (Gaussian kernel)	11.767	12.04
Decision Tree Regression	11.767	11.462

VII. MODELS AND RESULTS

Reression Model Evaluation Summary

In our regression analysis, the goal was to predict the potential sale prices of houses based on a set of features. Here's a summary of our findings:

i. Linear Regression (Baseline Model)

- Utilized 81 features and 1461 training samples.
- Accuracy Score: 88.82.

ii. Linear Regression with Lasso Regularization:

- Applied Lasso regularization after 5- fold cross-validation.
- Accuracy Score: 78.56.
- Automatically selected 56 variables and eliminated 35 variables.

iii. Linear Regression with Ridge Regularization:

- Applied Ridge regularization with cross-validation.
- Accuracy Score: 88.83.
- Improved performance over the baseline model, indicating regularization helped with overfitting.

iv. Support Vector Regression (SVR) with Gaussian Kernel:

- Utilized SVR with Gaussian kernel, cross-validating parameters.
- Generated a score of 11.138.

v. Random Forest Regression:

- Applied Random Forest Regression with max_depth parameter cross- validated to 150.
- Accuracy Score: 89.56.
- Outperformed the baseline model, showcasing better predictive power.

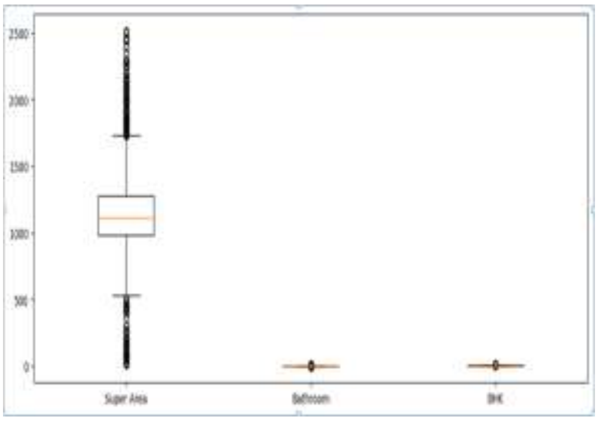
vi. Decision Tree Classifier:

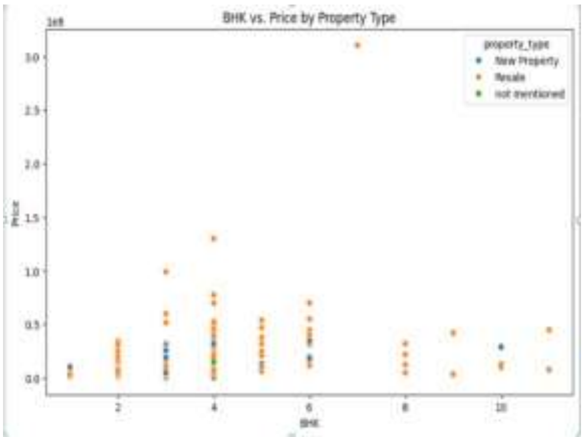
- Applied Decision Tree Classifier to the dataset.
- Accuracy Score: 79.56.

Random Forest Classifier demonstrated the highest accuracy score among the models.

Recommending the Random Forest Classifier for future house price predictions due to its superior performance in this analysis. This regression model evaluation provides insights into the effectiveness of different models in predicting house prices. The Random Forest Classifier stands out as the most accurate and reliable choice for future predictions.

VIII. VISUALIZATIONS AND ANALYSIS





This histogram depicts the property type and BHK style with respect to the price range.

IX. CONCLUSION

In conclusion, the proposed system effectively addresses existing issues in the current model for predicting house prices. Through comprehensive training and testing of datasets with various models, it is evident that both the Random Forest Classifier and Ridge Classifier outperform the simple linear regression model. Notably, the Random Forest Classifier achieved the highest accuracy score.

Key Points:

a. Improved Performance:

Random Forest Classifier and Ridge Classifier models demonstrated better accuracy compared to the baseline linear regression model.

b. Top Performer:

The Random Forest Classifier achieved the highest accuracy score among all models tested.

c. Recommendation:

We strongly recommend using the Random Forest Classifier for future house price predictions.

d. Outcome:

The project's outcome is the accurate prediction of house prices, benefiting both customers and developers.

In essence, the proposed system enhances accuracy and reliability in predicting house prices, providing a valuable tool for stakeholders involved in real estate. The adoption of the Random Forest Classifier is a strategic choice for achieving the best predictive outcomes in future applications.

X. REFERENCE:

[1] “Predicting Sales Prices of the Houses Using Regression Methods of Machine Learning”

[2] “ModelingHouse Price Prediction using Regression Analysis and ParticleSwarmOptimization”, (IJACS) International Journal of Advanced Computer Science and Applications, published in 2017.

[3] “Prediction of Real Estate Price Variation Based on Economic Parameters” Proceedings of the 2017IEEE International Conference on Applied System Innovation IEEE- ICASI 2017 - Meen, Prior & Lam (Eds).

[4] “Waiting to be Sold: Prediction of Time-Dependent House Selling Probability”,2016IEEE International Conference on Data Science and Advanced Analytics.

Navigating the Frontier : Challenges and it's Measures of Artificial Super Intelligence (ASI)

E.Likhitha, 23CSC02, Student,
M.Sc.(Computer Science)
Dept. of Computer Science
P.B.Siddhartha College of Arts &Science, Vijayawada, A.P, India
likhithaetukuri7@gmail.com

Hari Manasa Ganganagunta
Application Development Advisor
Cigna, Virgina, USA
ghariweb@gmail.com

Dr.S.Babu Rajendra Prasad,
Asso. Professor,
Dept. of Business Administration,
P.B.Siddhartha College of Arts & Science, A.P, India
rajendraprasad@pbsiddhartha.ac.in

ABSTRACT: The Field of Artificial Intelligence (AI) Has Shown an Upward Trend of Growth in the 21st Century (From 2000 To 2015). The Evolution in AI Has Advanced the Development of Human Society in Our Own Time, With Dramatic Revolutions Shaped by Both Theories and Techniques. However, The Multidisciplinary and Fast-Growing Features Make AI a Field in Which It Is Difficult to Be Well Understood. In This Paper, We Study About the Artificial Super Intelligence (ASI) How It Took the Part of The World, What Are It Risks or Challenges and How We Are Going to Reduce It. We Find That the Area Is in The Sustainable Development and Its Impact Continues to Grow. From the Perspective of Reference Behavior, The Decrease in Self-References Indicates That the AI Is Becoming More And More Open-Minded.

This Article Contributes to The Unending Conversation on Super intelligent AI by Shedding Light on The Moral Challenges and Proposing Actionable Strategies for Responsible Development. As the Field Evolves, An Ethical Framework Will Be Pivotal in Harnessing the Potential Benefits of Super AI While Mitigating Its Ethical Risks.

KEYWORDS: Weaponization, Super Intelligence, Devasting.

I. INTRODUCTION

Artificial Intelligence (AI) has grown dramatically and becomes more and more institutionalized in the 21st Century. In this era of interdisciplinary science, of computer science, cybernetics, automation, mathematical logic, and linguistics [1], questions have been raised about the specific concept of AI [2]. Actually, as early as the 1940s and 1950s, scientists in the field of Mathematics, Engineering, and Computer Science had explored the possibilities of artificial brains and were trying to define the intelligence of the machine [3]. Artificial intelligence (AI) has witnessed remarkable advancements in recent years, but the concept of Artificial Super Intelligence (ASI) takes the capabilities of AI to an entirely different level. ASI represents a hypothetical future stage of AI development where machines possess cognitive abilities far surpassing those of humans. While we have yet to achieve ASI, it is a topic that captivates the imagination of researchers, scientists, and enthusiasts alike [4]. In this article, we will explore the concept of artificial Super Intelligence, its potential implications, and the ethical considerations surrounding its development.

Fig.1.Artificial Intelligence (AI) Technology

Moreover, Artificial Super Intelligence, often abbreviated as ASI, is a term used to describe a level of AI development where machines can outperform humans in virtually every intellectual task [5].

It represents a point at which AI systems possess not only superior computational abilities but also exhibit higher-order cognitive functions, such as creativity, emotional intelligence, and self-awareness. ASI would be capable of rapid self-improvement, resulting in an exponential increase in its intelligence and problem-solving capabilities [6].

II. RELATED WORK

Risks in Super AI:

1) Loss of control and understanding:

One potential danger of super intelligence that has received a lot of attention from experts worldwide is that ASI systems could use their power and capabilities to carry out unforeseen actions, outperform human intellect, and eventually become unstoppable [7]. Advanced computer science, cognitive science, nanotechnology, and brain emulations have achieved greater-than-human machine intelligence. If something goes wrong with any one of these systems, we won't be in a position to contain them once they emerge. Moreover, predicting the system's response to our requests will be very difficult. Loss of control and understanding can thus lead to the destruction of the human race altogether [8].

2) The weaponization of super AI:

Today, it seems logical enough to think that highly advanced AI systems could potentially be used for social control or weaponization. Governments around the world are already using AI to strengthen their military operations. However, the addition of weaponized and conscious super intelligence could only transform and impact warfare negatively. Additionally, if such systems are unregulated, they could have dire consequences. Superhuman capabilities in programming, research & development, strategic planning, social influence, and cyber security could self-evolve and take positions that could become detrimental to humans [9].

3) Failure to align human and AI goals:

Super AI can be programmed to our advantage, however, there lies a non-zero probability of super AI developing a destructive method to achieve its goals. Such a situation may arise when we fail to align our AI goals [10].

4) Malevolent super intelligence:

The successful and safe development of AGI and super intelligence can be ensured by teaching it the aspects of human morality. However, ASI systems can be exploited by governments, corporations, and even sociopaths for various reasons, such as oppressing certain societal groups. Thus, super intelligence in the wrong hands can be devastating [11].

5) The danger of nuclear attacks:

With ASI, autonomous weapons, drones, and robots could acquire significant power. The danger of nuclear attacks is another potential threat of super intelligence. Enemy nations can attack countries with technological supremacy in AGI or superintelligence with advanced and autonomous nuclear weapons, ultimately leading to destruction [12].

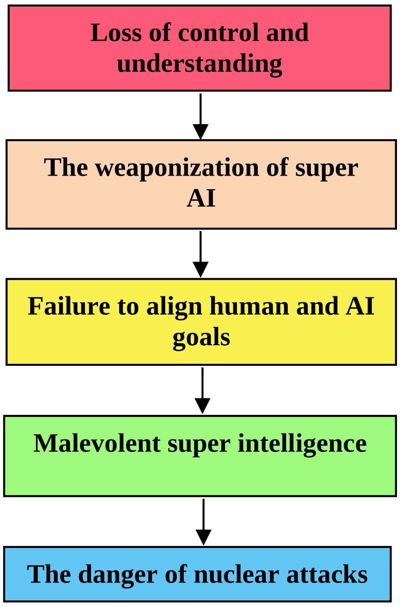

Loss of control and understanding
The weaponization of super AI
Failure to align human and AI goals
Malevolent super intelligence
The danger of nuclear attacks

Fig.2.Various risks in Super AI

III. PROPOSED WORK

We propose the following security methods to safeguard the Super AI Technology from various security attacks.

Measures to overcome from security risks of Super AI:

1. Robust AI safety research:

Investing in research to ensure the development of safe and reliable AI systems is crucial. This includes studying the potential risks, developing safety measures, and creating frameworks for AI systems to adhere to ethical guidelines.

2. Transparent and explainable AI:

Promoting transparency in AI algorithms and decision-making processes can help us understand how AI systems arrive at certain conclusions. This allows for better oversight and helps prevent unintended consequences.

3. International collaboration:

Encouraging global cooperation among researchers, policymakers, and industry leaders can foster a collective effort in addressing super AI threats. Sharing knowledge, best practices, and establishing common standards can help mitigate risks effectively.

4. Regular audits and regulations:

Implementing regular audits and robust regulatory frameworks can ensure that AI systems are designed, developed, and deployed in a responsible manner. This can help prevent misuse and minimize potential risks.

5. Ethical guidelines and safeguards:

Establishing clear ethical guidelines and safeguards for AI development can help ensure that AI systems are aligned with human values and respect fundamental rights. These guidelines should cover areas such as privacy, bias, and accountability.

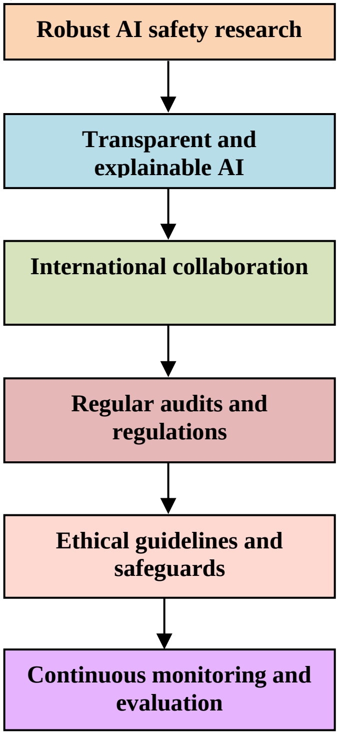

Robust AI safety research
Transparent and explainable AI
International collaboration
Regular audits and regulations
Ethical guidelines and safeguards
Continuous monitoring and evaluation

Fig .3. Various measures to reduce risks in Super AI

6. Continuous monitoring and evaluation:
Regularly monitoring and evaluating AI systems can help identify any potential risks or unintended consequences. This allows for timely interventions and improvements to mitigate any emerging threats.

ALGORITHM:

1. Begin
2. Identify potential Super AI
3. Focus on the Most Portable Threats that could harm resources.
4. Determine Security measures to protect resources
5. Put in place measures to efficiently protect resources
6. Assess the level of security to prevent unauthorized access.

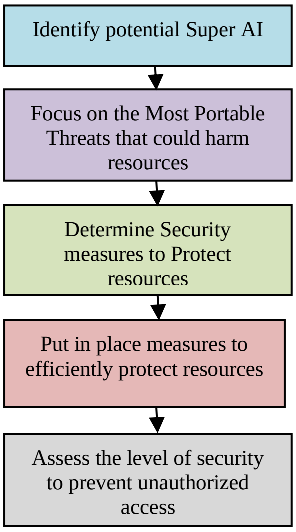

Identify potential Super AI
Focus on the Most Portable Threats that could harm resources
Determine Security measures to Protect resources
Put in place measures to efficiently protect resources
Assess the level of security to prevent unauthorized access

Fig.4.Procedure to protect resources of Super AI

IV. RESULT & ANALYSIS

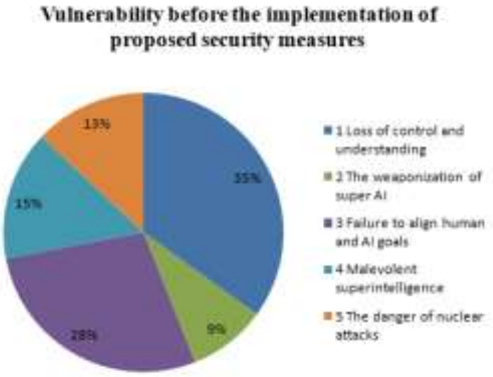


Fig.5.Enhancement of security before implementing the measures

S.No	Types of Attacks possible on Super AI Technology before implementing the security measures	Percentage of vulnerability
1	Loss of control and understanding	35
2	The weaponization of super AI	9
3	Failure to align human and AI goals	28
4	Malevolent superintelligence	15
5	The danger of nuclear attacks	13
Vulnerability before the implementation of Proposed Security Measures		100

Table 1. Types of possible Attacks on Super AI Technology before implementing the Security Measures.

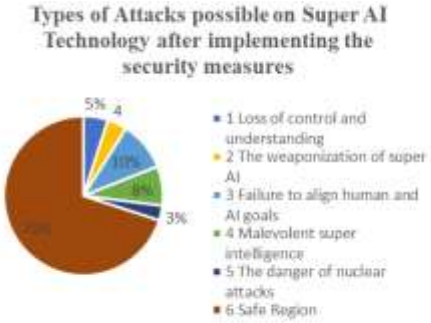


Fig.6.Enhancement of security after implementing the security measures

S.No	Types of Attacks possible on Super AI Technology after implementing the security measures	Percentage of vulnerability
1	Loss of control and understanding	5
2	The weaponization of super AI	4
3	Failure to align human and AI goals	10
4	Malevolent superintelligence	8
5	The danger of nuclear attacks	3
Vulnerability before the implementation of Proposed Security Measures		30

Table 2. Types of possible Attacks on Super AI Technology after implementing the Security Measures.

After implementation of the proposed security measures we have controlled most of the security attacks from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even through several security measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of Super AI Technology. Hackers introduces are continuously making attempt to gain the unauthorized access of Super AI using various attacks. As Super AI technology has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Super AI Technology several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] D. Vernon, G. Metta and G. Sandini, "A survey of artificial cognitive systems: Implications for the autonomous development of mental capabilities in computational agents", IEEE Trans. Evol. Comput., vol. 11, pp. 151-180, Apr. 2007.

[2] D. Kirsh, "Thinking with external representations", *Ai Soc.*, vol. 25, no. 4, pp. 441-454, 2010.

[3] Bostrom, Nick (2002), "Existential Risks", Journal of Evolution and Technology, **9**, retrieved 2007-08-07

[4] Gouveia, Steven S., ed. (2020). "ch. 4, "Humans and Intelligent Machines: Co-evolution, Fusion or Replacement?", David Pearce". The Age of Artificial Intelligence: An Exploration. Vernon Press. ISBN 978-1-62273-872-4.

[5] Joy, Bill (April 1, 2000). "Why the future doesn't need us". Wired. See also technological singularity. Nick Bostrom 2002 Ethical Issues in Advanced Artificial Intelligence.

[6] Legg, Shane (2008). Machine Super Intelligence (PDF) (PhD). Department of Informatics, University of Lugano. Retrieved September 19, 2014.

[7] Roman V. Yampolskiy and M. S. Spellchecker, Artificial Intelligence Safety and Cybersecurity: A Timeline of AI Failures, [online] Available: https://arxiv.org/pdf/1610.07997.

[8] Ford, K. M. (1989) A constructivist view of the frame problem in artificial intelligence. Canadian Psychology, 30: 188 – 190.

[9] Armitage.R.(2019) We must oppose lethal autonomous weapon systems. Br.J.Gen.pract 69, 510-511.doi.10_3399/bjgp19X705869.

[10] Russell, Stuart J.; Norvig, Peter (2021). Artificial intelligence: A modern approach (4th ed.). Pearson. pp. 5, 1003. ISBN 9780134610993. Retrieved September 12, 2022.

[11] Millar, Isabel (October 2020). The Psychoanalysis of Artificial Intelligence (PDF) (PhD thesis). Kingston School of Art. doi:10.1007/978-3-030-67981-1. ISBN 978-3-030-67980-4. Archived (PDF) from the original on 18 May 2022. Retrieved 20 October 2022.

[12] Papernot, N., P. McDaniel, and I. Goodfellow, "Transferability in Machine Learning: from Phenomena to Black-Box Attacks Using Adversarial Samples," arXiv, May 24, 2016. As of August 15, 2017: https://arxiv.org/abs/1605.0727

Quantum Computing : Unraveling the Risks and Safeguarding the Future

G.Pavan
23CSC03, Student, M.Sc.(Computer Science)
Department of Computer Scince
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
pavan.ganugupati97016@gmail.com

V.Rama Krishna
23CSC25, Student, M.Sc.(Computer Science)
Department of Computer Scince
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
ramakrishnamadi1020@gmail.com

P. Satya Naga Vara Prasad
23CSC15, Student, M.Sc.(Computer Science)
Department of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India.
Satyaprasadpujari3699@gmail.com

ABSTRACT: **Quantum Computing Is A Type of Computing That Leverages the Principles of Quantum Mechanics, Such as Superposition and Entanglement, To Perform Operations on Data. Unlike Classical Computers That Use Bits to Represent Either A 0 Or A 1, Quantum Computers Use Qubits, Which Can Exist in Multiple States Simultaneously. This Allows Quantum Computers to Process Information in Parallel, Potentially Solving Certain Problems Much Faster Than Classical Computers. However, Building Practical and Stable Quantum Computers Is A Complex Scientific and Engineering Challenge That Is Still in The Early Stages of Development. Quantum Computing Harnesses the Principles of Quantum Mechanics to Process Information Using Qubits, Which Can Exist in Multiple States Simultaneously. This Enables Parallel Computation, Potentially Solving Specific Problems Exponentially Faster Than Classical Computers. Despite the Promise, Practical Implementation Faces Formidable Challenges, And Ongoing Research Seeks to Overcome Issues Like Decoherence And Error Correction for the Realization of Robust Quantum Computers.**

KEYWORDS: Scalability, Decoherence, Network, Security, Topological.

I. INTRODUCTION

Quantum computers aren't constrained to two states; they encode data as quantum bits, or qubits, where bits can be 0 or 1 or both 0 and 1 at the same time in what is called super position. The similarity of silicon qubits with CMOS foundries is an extraordinary resource. Quantum computers utilizing the property of superposition can process and store multiple states simultaneously, thus ensuring it's potential to be millions of times extra dominant than today's most brand influential supercomputers. Moreover, quantum computers guarantee secure transmission, ultrahigh speed and ability to store large amount of information than its classical counterparts.[1] Quantum Computing is a completely new model of computation based on the laws of quantum physics. It is not an improvement or extension of the current classical digital computing model that has been used for many years, but it is the first time in history that computing is branching. Significant resources are invested worldwide, and we are at the beginning of a new age of computation, developing programmable quantum systems towards universal quantum computers. Quantum computers promise to solve certain mathematical problems that are intractable to classical computers [2]. By using the physical phenomena of superposition, entanglement and interference, quantum computers can solve problems computationally hard for even the most advanced classical computers. Quantum entanglement creates strong correlations between qubit states leading to increased information in the combined system compared with the individual. Quantum Computing is the only way to enlarge the computational space and access this unique resource which cannot be mimicked by classical computing as it would require exponential resources. Quantum computing has become a reality.

Quantum computers are available to everybody via cloud service or simulation. Toolkits are available that invite practitioners to start their own quantum software projects and thus get used to this novel technology [3]. In this article we evaluate technologies to help developers to start their own quantum software business. Practical guidance is provided from our own quantum technology projects. Quantum Computing (QC) has been a theoretical promise since the beginning of 1990‘s. A lot of research effort has been invested, especially in two areas. First, on the mathematics, logics and algorithms area. Second, quantum physicist and materials experts have been working on how to implement such a machine.[4] In the last years the importance of quantum computing has significantly increased due to both continuously shrinking of the size of silicon-based integrated circuits and the results in quantum algorithm development. Quantum computing offers a path forward by taking advantage of quantum mechanical properties. So, the rapid progress of computer science led to a corresponding evolution of computation from classical computation to quantum computation.[5] In general, quantum computers can be broadly classified into universal gate quantum computers and quantum annealers. The universal gate quantum computer/processor can be seen as a quantum counterpart to a classical general purpose microprocessor, where IBM (127 qubit), Google (72 qubit) are in rapid pursuit of building faster and larger universal gate based quantum computers. On the other hand, the quantum annealers are akin to Application-Specific IC (ASIC), which can be used for solving a specific set of combinatorial optimization problems over discrete search space. However, the problems of interest in the domain of security primarily eyes the growth of universal quantum computers, which is not polynomial equivalent to quantum annealer [6]. Quantum computing has been a very active and promising area of research and, especially in the last years, of technology development. Since the physicist Richard Feynman proposed the idea of building a quantum computer to simulate quantum systems in the early 80's, several quantum algorithms and quantum error correction techniques have been developed. By exploiting quantum phenomena such as superposition and entanglement, quantum computers promise to solve hard problems that are intractable for even the most powerful conventional supercomputers. In addition, remarkable progress has been made in quantum hardware based on different technologies such as superconducting circuits, trapped ions, silicon quantum dots, and topological qubits. A recent breakthrough in quantum computing has been the experimental demonstration of quantum supremacy using a superconducting quantum processor consisting of 53 qubits [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in Quantum Computing:

Risks in Quantum Computing:

1) Security Risks: Shor's Algorithm Quantum computers have the potential to efficiently solve certain mathematical problems, such as factoring large numbers. Shor's algorithm, for example, could threaten the security of widely used encryption algorithms (RSA and ECC), which rely on the difficulty of factoring large numbers for their security [8].

2) Data Security: Quantum Key Distribution (QKD) While quantum computing poses a threat to classical cryptographic systems, it also offers new solutions like Quantum Key Distribution (QKD) for secure communication. However, the practical implementation of QKD is still in its early stages, and there are challenges to overcome in terms of scalability and reliability [9].

3) Decoherence: Quantum systems are prone to decoherence, where the delicate quantum state is disrupted by external factors. Maintaining the coherence of qubits over extended periods is crucial for the reliability of quantum computations. [10].

4) Scalability: Scaling up quantum computers to handle practical problems requires overcoming numerous technical hurdles. As the number of qubits increases, maintaining coherence and managing errors become even more challenging [11].

5) Security Threats: The advent of powerful quantum computers may lead to new forms of cyber threats and vulnerabilities. Governments, organizations, and individuals need to be prepared for potential misuse of quantum technology for malicious purposes [12].

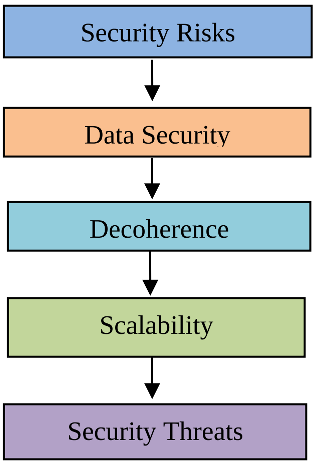


Fig. 3. Risks to Quantum Computing

III. PROPOSED WORK

We propose the following security methods to prevent threats on Quantum Computing.

1) Quantum Speedup: Quantum speedup refers to the advantage that a quantum algorithm has over its classical counterparts. It is often expressed as the ratio of the time taken by a classical algorithm to solve a problem compared to the time taken by a quantum algorithm.

2) Algorithmic Complexity: Just as in classical computing, quantum computing has its own algorithms and computational complexity classes. Understanding the algorithmic complexity of quantum algorithms helps in assessing their efficiency for specific tasks.

3) Topological Quantum Computing: Topological quantum computing is a theoretical approach that uses anyons, exotic particles with fractional quantum statistics, as qubits. The advantage is that these qubits are more robust against certain types of errors.

4) Adiabatic Quantum Computing: Adiabatic quantum computing involves the gradual transformation of a quantum system from an easily prepared initial state to a final state that represents the solution to a computational problem. It is an alternative quantum computing model to gate-based quantum computing.

5) Hybrid Quantum-Classical Systems: Hybrid quantum-classical systems combine quantum processors with classical computing resources to tackle problems that might be beyond the capabilities of either approach alone. This hybrid model aims to leverage the strengths of both quantum and classical computing.

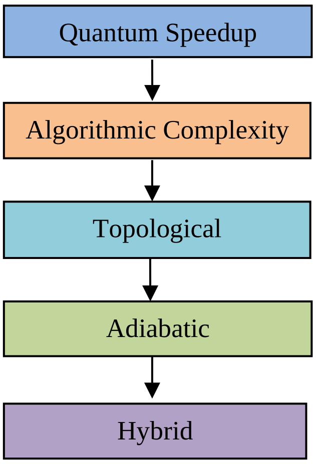


Fig. 3. Measures to Quantum Computing

Algorithm:

1. Begin
2. Identify Potential Fog Computing Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End

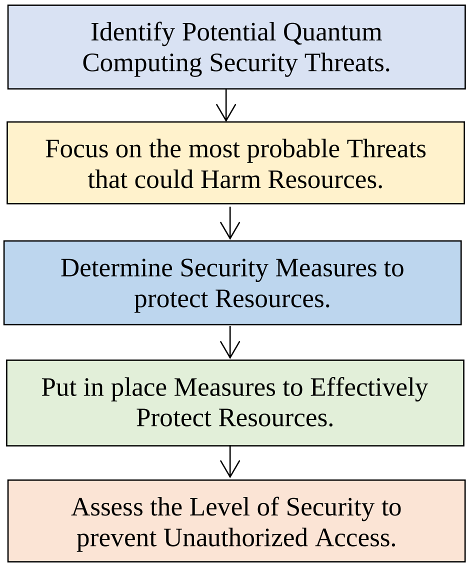

Identify Potential Quantum Computing Security Threats.
Focus on the most probable Threats that could Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 4. Procedure to safeguard the resources of Quantum Computing.

IV. RESULT & ANALYSIS

S. No	Types of Attacks possible on Quantum Computing Technology before implementing the Security Measures	Percentag e of Vulnerabi lity
1	Security Risks	21
2	Data Security	19
3	Decoherence	18
4	Scalability	22
5	Security Threats	20
Vulnerability before the implementation of proposed Security Risks		100
Table 1. Types of Possible Attacks on Quantum Computing before implementing the Security Measures		

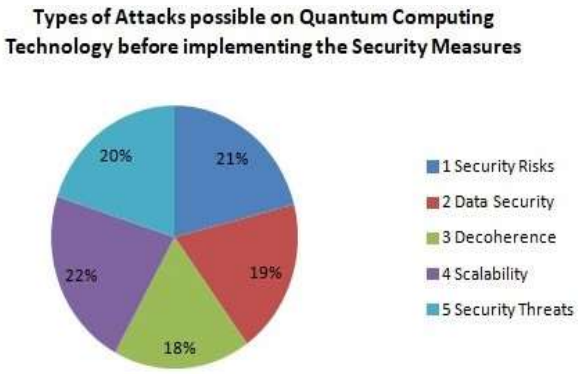


Fig. 1. Risk in quantum computing before implementing the Security Measures.

S. No	Types of Attacks possible on Quantum Computing Technology after implementing the Security Measures	Percentag e of Vulnerabi lity
1	Security Risks	10
2	Data Security	5
3	Decoherence	7
4	Scalability	3
5	Security Threats	5
Vulnerability after the implementation of proposed Security Measures		30
Table 1. Types of Possible Attacks on Quantum Computing after implementing the Security Measures		

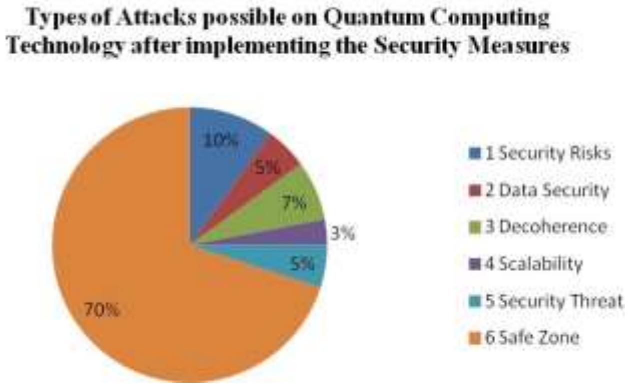


Fig. 1. Risk in quantum computing after implementing the Security Measures.

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of Quantum Computing. Hackers/ introduces are continuously making attempts to gain the unauthorized access of Quantum Computing using various attacks.

Quantum Computing devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Quantum Computing several new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Hilal Ahmad Bhat et.al, “Quantum Computing: Fundamentals, Implementations and Applications”, 27 May 2022, Electronic ISSN: 2644-1292,DOI: 10.1109/OJNANO.2022.3178545.

[2] H.Riel et.al,Quantum Computing Technology”,09 March 2022,DOI:10.1109/IEDMI19574.2021.9720538,Electronic ISBN: 978-1-6654-2572-8.

[3] Jose Luis Hevia et.al, “Quantum Computing”, 20 August 2021 , DOI: 10.1109/MS.2021.3087755, Electronic ISSN: 1937-4194.

[4] Rafael Sotelo et.al, “Quantum Computing What Why Who”, 10 February 2020, DOI: 10.1109/CHILECON47746.2019.8988080, Electronic ISBN:978-1-7281-3185-6.

[5] Adina Bărîlă et.al, “From Classical Computing to Quantum Computing”, 15-17 May 2014, DOI: 10.1109/DAAS.2014.6842455, Electronic ISBN:978-1-4799-5094-2.

[6] Prasanna Ravi et.al, “Security And Quantum Computing An Overview”, 08 September 2022, DOI: 10.1109/LATS57337.2022.9936966, Electronic ISBN:978-1-6654-5707-1.

[7] Carmen G. Almudever et.al, “Realizing Quantum Alogorithms On Real Quantum Computing Devices”, 09-13 March 2020, DOI: 10.23919/DATE48585.2020.9116240, Electronic ISBN:978-3-9819263-4-7.

[8] Nouioua Tarek et.al, “The Quantum Computer and the Security of Information Systems”, 22 September 2021, DOI: 10.1109/ICRAMI52622.2021.9585929, Electronic ISBN:978-1-6654-4171-1.

[9] Abhinav Dwivedi et.al, “Cyber Security and Prevention in the Quantum Era”, 05 March 2023
DOI: 10.1109/INOCON57975.2023.10101186, Electronic ISBN:979-8-3503-2092-3.

[10] M. Adeeb Ghonaimy et.al, “Quantum Network Security”, 16 December 2009, DOI: 10.1109/ICCES.2009.5383322.

[11] M. Vinet et.al, “Towards Scalable Silicon Quantum Computing”, 05 December 2018, DOI: 10.1109/IEDM.2018.8614675, Electronic ISBN:978-1-7281-1987-8.

[12] Hemant Bhatt et.at, “Quantum Computing: A New Era Of Computer Science”, 15 March 2019, Electronic ISBN:978-9-3805-4434-2.

Impacts of Artificial Intelligence : Risks to Measures from Artificial Intelligence

BHARGAV GUJJALA
23CSC06, Student, M.Sc(Computer Science)
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
bhargavgujjala@gmail.com

DHANUNJAY MADDALI
23CSC34, Student, M.Sc.(Computer Science)
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India.
maddalidhanunjay111@gmail.com

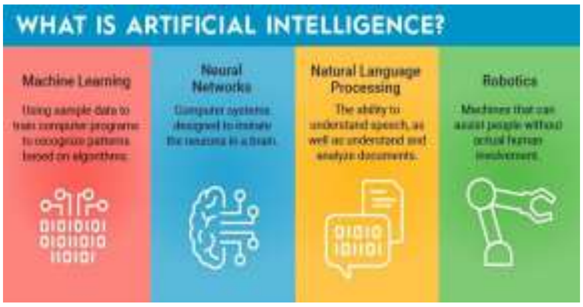
LOKESH CHAKKA
23CSC19, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India.
chakkalokesh2002@gmail.com

ABSTRACT: Artificial Intelligence is the Simulation of Human Intelligence Process by Machines, Especially Computer Systems. Specific Applications of AI Include Expert Systems, Natural Language Processing, Speech Recognition and Machine Vision. The Field of Artificial Intelligence (AI) Has Shown an Upward Trend of Growth in the 21st Century (From 2000 To 2015). The Evolution in AI Has Advanced the Development of Human Society in Our Own Time, With Dramatic Revolutions Shaped by Both Theories and Techniques Online Social Media (OSM) Has Become an Integral Part of An Individual's Daily Life. The Extensive Computational Power and Decision-Making Ability of Artificial Intelligence (AI) And the Proliferation of User-Generated Data on OSM Have Made the Opinion One of The Key Emerging Research Areas. However, The Ease of Accessing, Manipulating, And Mining Such User- Generated Data Raises Concerns About Privacy and Security, Data and Algorithmic Biases and Fairness. Nevertheless, Their Personal and Societal Implications Are Barely Addressed. This Article Discusses Various Types of Attacks That Intruders or Hackers Can Carry Out to Gain Unauthorized Access Over Artificial Intelligence Technologies. It Also Presents Measures to Minimize These Attacks on Resources of AI Technologies in Finance. The Article Conducts A Thorough Examination of The Likelihood of Security Threats and Explores Various Ways to Minimize the Risks of Hacking, Providing Recommendations to Enhance Security.

KEYWORDS: Security, Authentication, Penetrates, Digital, Disciplines.

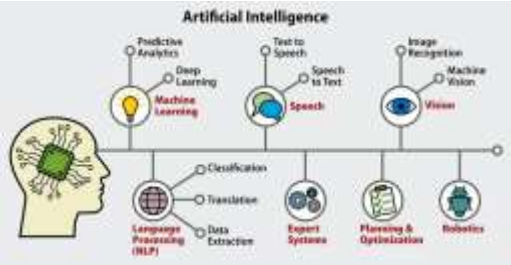
I. INTRODUCTION

Artificial Intelligence has achieved rapid and remarkable development during the last decade. AI technologies such as machine learning (ML), natural language processing, and computer vision are increasingly permeating and spreading to various disciplines and aspects of our society [7]. AI is increasingly taking over human tasks and replacing human decision-making. It has been widely used in a variety of sectors, such as business, logistics, manufacturing, transportation, health care, education, state governance, etc. The application of AI has brought about efficiency improvement and cost reduction, which are beneficial for economic growth, telemedicine services. It is no doubt that the rapid development and wide application of AI are already affecting our daily life, humanity, and society. However, at the same time, AI also poses many significant ethical risks or issues for users, developers, humans, and society. Over the past few years, many cases in which AI produced poor outcomes have been observed. For instance, in 2016, the driver of an electric Tesla car was killed in a road accident after its Autopilot mode failed to recognize an oncoming lorry [2]. The rapid, widespread implementation of artificial intelligence technologies in workplaces has implications for business communication. In this article, the authors describe current capabilities, challenges, and concepts related to the adoption and use of artificial intelligence (AI) technologies in business communication. Understanding the abilities and inabilities of AI technologies is critical to using these technologies ethically. [3]. In the digital era, cyber security has become a serious problem. Information penetrates, wholesale fraud, manual human test breaking, and other comparable occurrences proliferate, influencing a large number of individuals just as organizations [4].


WHAT IS ARTIFICIAL INTELLIGENCE?
Machine Learning
Using sample data to train computer programs to recognize patterns based on algorithms.
Neural Networks
Computer systems designed to imitate the neurons in a brain.
Natural Language Processing
The ability to understand speech, as well as understand and analyze documents.
Robotics
Machines that can assist people without actual human involvement.

AI ethics is an important emerging topic among academia, industry, government, society, and individuals. In the past decades, many efforts have been made to study the ethical issues in AI. [5] The main findings are:

This article offers a comprehensive overview of the AI ethics field, including a summary and analysis of AI ethical issues, ethical guidelines and principles, approaches to address AI ethical issues, and methods to evaluate the ethics of AI technologies.[9]. In the digital era, cyber security has become a serious problem. Information penetrates, wholesale fraud, manual human test breaking, and other comparable occurrences proliferate, influencing a large number of individuals just as organizations.[8]. In the digital era, cyber security has become a serious problem. Information penetrates, wholesale fraud, manual human test breaking, and other comparable occurrences proliferate, influencing a large number of individuals just as organizations.[6]. We find that over-reliance or authoritative stigmatization is present when AI is concerned and that with human guidance discursive explanatory decision-making is present. We conclude that while AI is seen as authoritative even in a low stake decision-making setting, it does not suppress choice, but combined with a lack of transparency, AI suppresses visibility into rationality creation by the decision maker. Based on the emergent explorative relationships between types of rationality, AI transparency and authoritativeness, we provide future research avenues based on our findings [10][11].



II. RELATED WORK

Security Risks and Challenges of Artificial Intelligence:

1) Bias and Fairness

Issue: AI systems can inherit biases from the data they are trained on, leading to discriminatory outcomes. Biases present in historical data can perpetuate social inequalities. **Mitigation:** Strive for diverse and representative training data, implement bias detection tools, and regularly audit AI systems for fairness.

2) Job Displacement

Issue: Automation and AI may replace certain jobs, leading to unemployment and the need for workers to adapt to new skill requirements.

Mitigation: Invest in education and training programs to equip the workforce with the skills needed for the evolving job market.

3) Security Concerns

Issue: AI systems can be vulnerable to adversarial attacks, where malicious actors manipulate input data to deceive the system.

Mitigation: Implement robust cyber security measures, conduct regular security audits, and develop AI systems with adversarial robustness in mind.

4) Ethical Use

Issue: The potential for AI to be used unethically, such as in surveillance, social manipulation, or autonomous weapons. **Mitigation:** Establish clear ethical guidelines, adhere to regulations, and ensure responsible use of AI technologies.

5) Lack of Transparency

Issue: Some AI algorithms, especially in deep learning, are often considered "black boxes" with opaque decision- making processes.

Mitigation: Promote transparency in AI systems, develop explainable AI techniques, and ensure accountability for the decisions made by AI.

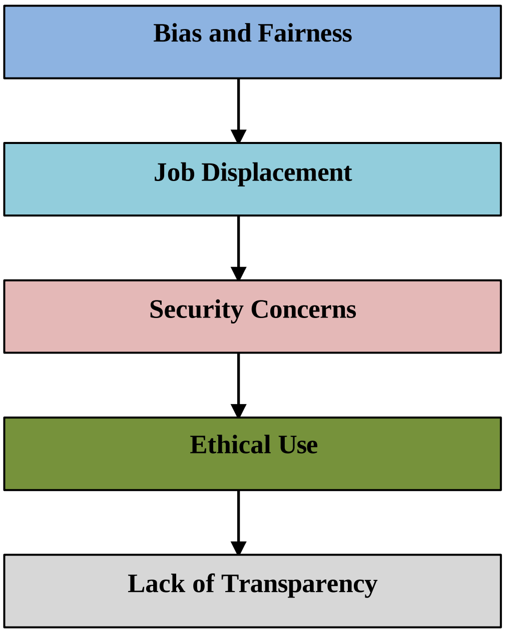


Fig 1. Various security risks in Artificial Intelligence.

III. PROPOSED WORK

We propose the following security methods to prevent Risks on Artificial Intelligence:

1) Data Security and Data Encapsulation

Encryption of Data: Implement robust encryption techniques to protect sensitive data during storage, processing, and transmission.

Access Control over data: Restrict and manage access to data, ensuring that only authorized personnel and systems can interact with sensitive information.

2) Model Security

Secure Development Practices: Follow secure coding practices during the development of AI models to minimize vulnerabilities.

Regular Audits and Testing: Conduct regular security audits and testing, including penetration testing, to identify and address potential weaknesses.

3) Adversarial Robustness

Adversarial Training: Train AI models with adversarial examples to enhance their robustness against adversarial attacks.

Robust Architecture Design: Develop AI models with architectures that are inherently resilient to adversarial manipulations.

4) Secure Deployment program

Containerization: Use containerization technologies to isolate AI models and their dependencies, enhancing security and scalability.

Secure APIs: Implement secure Application Programming Interfaces (APIs) for communication between different components of AI systems.

5) Explain ability of AI and Transparency

Interpretable Models of AI: Prefer models that are more interpretable, allowing easier identification of potential security issues.

Model Monitoring and Risk Analysis: Continuously monitor the behavior of AI models in production to detect anomalies or unexpected patterns.

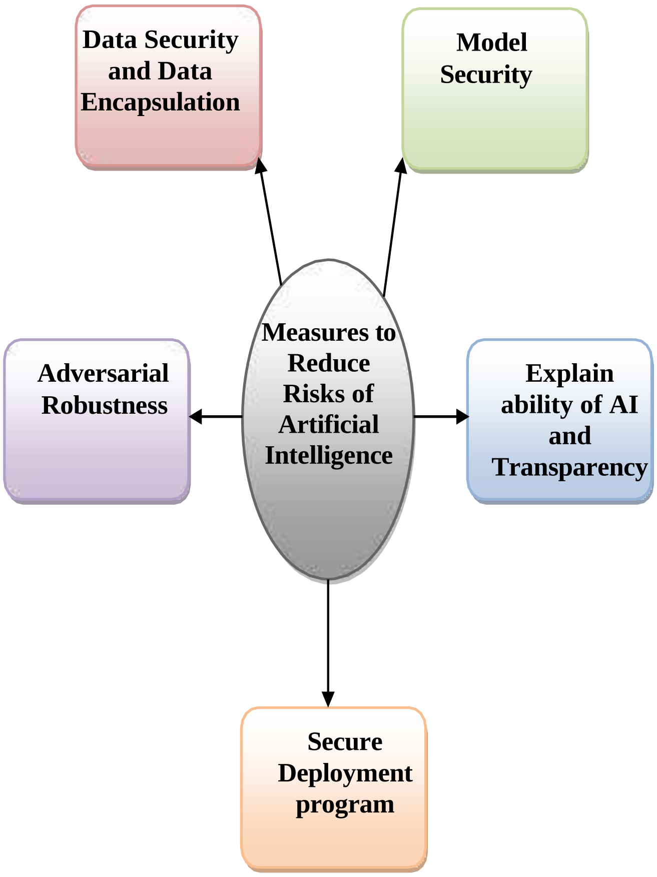

Data Security and Data Encapsulation
Model Security
Adversarial Robustness
Measures to Reduce Risks of Artificial Intelligence
Explain ability of AI and Transparency
Secure Deployment program

Fig 2. Various Measures to Reduce Risks of Artificial Intelligence

Algorithm:

1. Begin
2. Identify Potential Artificial Intelligence Security Threats.
3. Focus on the Most Probable Threats That Could Harm Resources.
4. Determine Security Measures to Protect Resources.
5. Put in Place Measures to Effectively Protect Resources.
6. Access the level of Security to Prevent Unauthorized access.
7. End

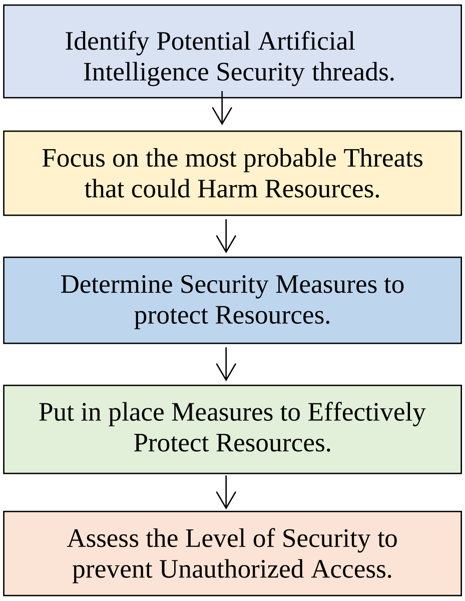

Identify Potential Artificial Intelligence Security threads.
Focus on the most probable Threats that could Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 4. Procedure to safeguard the resources of Artificial Intelligence.

IV. RESULT AND ANALYSIS

S.No	Types of Attacks possible on Artificial Intelligence before implementing the Security Measures	Percentage of Vulnerability
1	Bias and Fairness	4
2	Job Displacement	13
3	Security Concerns	18
4	Ethical Use	24
5	Lack of Transparency	41
Vulnerability before the implementation of proposed security measures		100

Table 1. Types of possible Attacks on Artificial Intelligence before implementing the Security Measures

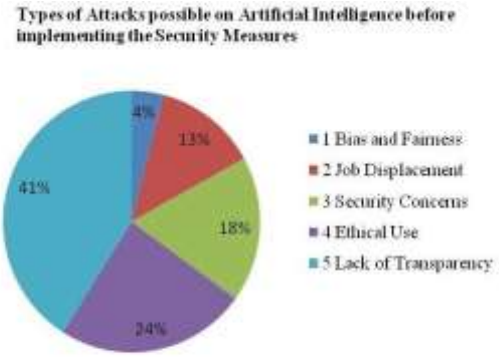


Fig 3. Types of possible Attacks on Artificial Intelligence before implementing the Security Measures

S.No	Types of Attacks possible on Artificial Intelligence after implementing the Security Measures	Percentage of Vulnerability
1	Bias and Fairness	2
2	Job Displacement	7
3	Security Concerns	3
4	Ethical Use	5
5	Lack of Transparency	10
Vulnerability after the implementation of proposed security measures		27

Table 2. Types of possible Attacks on Artificial Intelligence after implementing the Security Measures

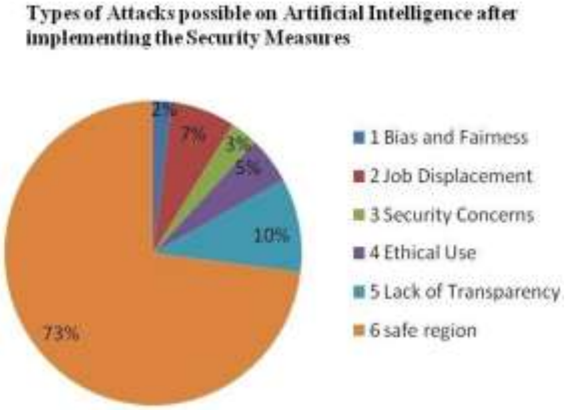


Fig 4. Types of possible Attacks on Artificial Intelligence after implementing the Security Measures

After implement the security measures we have restricted most of the security risks from 100% to 27%.

V. FUTURE WORK

1. Today, at every level of society, we are struggling with the question of how to live and work better together. Many individuals are struggling to find their footing amidst burnout, fake news, and flaring culture wars. Many organizations are struggling to reconfigure the workplace for a work-from-home future. Many societies are struggling to overcome vaccine refusal and the collapse of public trust.
2. How to live and work better together: it’s a complex question. Throughout most of human history, we’ve treated it as a philosophical or political debate. One side of this ancient debate has viewed our collective behavior (i.e., how we interact with one another) as something that self-corrects toward goodness, given the chance.
3. In his book Politics (4th-century BCE), Aristotle argued that all free people are born with the potential to become virtuous and wise. These good-natured qualities naturally come forth, given a healthy environment in which to develop proper habits and practical experience.
4. The other side of the debate has maintained that how we interact needs to be actively managed and guided by a strong hand. Otherwise, our bad-natured and chaotic qualities will run amok and ruin peace.
5. Hobbes expressed this view in his Leviathan (1651) : “In the State of Nature, without rules or contracts, the idea of fairness has no place and people are in a relentless game of survival.”
6. To Hobbes’ thinking, contracts between people would only be honored if backed up by the threat of force: “Covenants, without the sword, are but words and of no strength to secure a man at all.”
7. In an interdisciplinary paper that generated lots of conversation globally among big-name academics, Joseph Bak-Coleman, Mark Alfano, Wolfram Barfuss and many others advocate a paradigm shift. What if “how we should live and work together” is not a debate at all? What if it’s a result of natural selection?

We have a second, social brain. It evolved in us over millennia.

VI. CONCLUSION

Even though several security measures are implemented using protocols firewalls which are unable to protect the vulnerabilities of Artificial Intelligence. Hackers / Introduces are continuously making attempt to gain the unauthorized access of Artificial Intelligence using various attacks. As Artificial Intelligence usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Artificial Intelligence several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VII. REFERENCES

[1] Jiaying Liu, “Artificial Intelligence: Artificial Intelligence in the 21st Century”, IEEE, 26 March 2018, DOI:10.1109/ACCESS.2018.2819688, Electronic ISSN: 2169-3536.

[2] FAHIM ANZUM, “ARTIFICIAL INTELLIGENCE: BIASES, FAIRNESS, AND IMPLICATIONS OF USING AI IN SOCIAL MEDIA DATA MINING”, IEEE, 7 NOVEMBER 2022, DOI: 10.1109/CW55638.2022.00056.

[3] Kristen M. Getchel, “Artificial Intelligence in Business Communication: The Changing Landscape of Research and Teaching”, IEEE, 1 March 2022, DOI:10.1177/23294906221074311.

[4] A. Mehra, "Artificial Intelligence Enabled Cyber Security,", IEEE, 2021 6th,

DOI: 10.1109/ISPCC53510.2021.9609376.

[5] C. Huang, "An Overview of Artificial Intelligence Ethics,", IEEE, 25/Aug/2023,

DOI: 10.1109/TAI.2022.3194503.

[6] L. VALTONEN "EXPLORING THE RELATIONSHIPS BETWEEN ARTIFICIAL INTELLIGENCE TRANSPARENCY, SOURCES OF BIAS, AND TYPES OF RATIONALITY, IEEE, 25.FEB.2022, DOI:10.1109/IEEM55944.2022.9989994.

[7] MINGYUAN LIU, “LEARNING BASED ADAPTIVE NETWORK IMMUNE MECHANISM TO DEFENSE EAVESDROPPING ATTACKS”, IEEE, 29/NOVEMBER/2019, DOI: 10.1109/ACCESS.2019.2956805, ELECTRONIC ISSN: 2169-3536.

[8] DOOWON JEONG, “ARTIFICIAL INTELLIGENCE SECURITY THREAT, CRIME, AND FORENSICS: TAXONOMY AND OPEN ISSUES”, IEEE,

OCTOBER 7, 2020, DOI:10.1109/ACCESS.2020.3029280.

[9] JUNHAO DONG, “TOWARD INTRINSIC ADVERSARIAL ROBUSTNESS THROUGH PROBABILISTIC TRAINING”, IEEE, 10 JULY 2023,

DOI: 10.1109/TIP.2023.3290532.

[10] DALTON CÉZANE GOMES VALADARES

,” AUTOMATING THE DEPLOYMENT OF ARTIFICIAL INTELLIGENCE SERVICES IN MULTIACCESS EDGE COMPUTING SCENARIOS “, IEEE, 2 SEPTEMBER 2022

, DOI:10.1109/ACCESS.2022.3208118.

[11] K. LETRACHE AND M. RAMDANI, "EXPLAINABLE ARTIFICIAL INTELLIGENCE: A REVIEW AND CASE STUDY ON MODEL-AGNOSTIC METHODS”,2023 14TH INTERNATIONAL CONFERENCE ON INTELLIGENT SYSTEMS: THEORIES AND APPLICATIONS (SITA), CASABLANCA, MOROCCO, DOI: 10.1109/SITA60746.2023.10373722.

Security Standards on Cyber Security

J.Gopi, 23CSC07, Student,
M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts &
Science,Vijayawada, A.P, India.
gopi95117@gmail.com

Dr.T.Srinivasa Krishna,
Asst. Professor,
Dept. of Physics, P.B.Siddhartha
College of Arts & Science, A.P, India
tskrishna@pbsiddhartha.ac.in

Praneeth Chalamalasetti,
Software Engineer Senior Analyst,
Cigna, Virgina, USA.
p2neeth@gmail.com

ABSTRACT: As More Business Activities Are Being Automated and An Increasing Number of Computers Are Being Used to Store Sensitive Information, The Need for Secure Computer Systems Becomes More Apparent. This Need Is Even More Apparent as Systems and Applications Are Being Distributed and Accessed Via an Insecure Network, Such as The Internet. The Internet Itself Has Become Critical for Governments, Companies, Financial Institutions, And Millions of Everyday Users. Networks of Computers Support A Multitude of Activities Whose Loss Would All but Cripple These Organizations. As A Consequence, Cybersecurity Issues Have Become National Security Issues. Protecting the Internet Is A Difficult Task Cybersecurity Can Be Obtained Only Through Systematic Development; It Cannot Be Achieved Through Haphazard Seat-Of-The-Pants Methods. Applying Software Engineering Techniques to The Problem Is A Step in The Right Direction.

I. INTRODUCTION

In recent years, networks have evolved from a mere means of communication to a ubiquitous computational infrastructure. Networks have become larger, faster, and highly dynamic. The pervasive use of computer and network technologies in all walks of life has turned cyber security issues into national security issues [1].

Fig.1.Illustration on cyber security.

The setting in which companies run and how they conduct business have altered as a result of the fast spread of information systems. Their information technology (IT) systems are connected due to the increasing use of data and communications technologies [2]. History shows that the losses to the financial organization or individuals through criminal activities are multifold. Even the government and defence organization have experienced significant cyber losses and disruptions [3]. In present day culture, digital assaults are extending emphatically. intermediary apparatus. Cyber security is the blend of approaches and practices to forestall and screen PCs, organizations [4]. HSPD– 7, the NIPP, the DIB Plan, and the DoD 8000 series policies all address the need and requirements for risk management strategies [5]. Cyber Security is part of lives, when people go online, whether it's for shopping, communication or managing different accounts, not limited to first world countries such as Australia, Canada and the United States[6].The digital world is represented by the computer-based systems installed in the devices to enable full remote control via the Internet in terms of communication and data exchange [7].Cyber security in health care is a special concern since patient safety and confidentiality are at risk. It is typical for banks to cancel a stolen credit card number, issues new one with a new number, and repay the customer. The structure of technologies and procedures prepared to protect the data from malicious users. Though, the cyber data is never 100% safe from the cyber attacks. As the rapidly growing nature of 'Social media' users tend to become more easily caught by the cyber-attackers. It has been spotted that the social media platforms have become more popular these days. It may Generated Content" Facebook, twitter, WhatsApp, LinkedIn etc. have made communications very convenient between people which are online. As we all are aware that these online sites are a great source of communication and engagement with persons all over the globe, people also tend to post their sensitive information such as location, bank details etc.

II. RELATED WORK

In this section, we exemplify various Security Risks in cyber security

Risks in Fog Computing

1. Data breaches

A security breach involves unauthorized access to sensitive information, such as personal data. Cybercriminals target Data breaches can also be accidental [8].

2. Malware:

sensitive data to an internet-connected cloud environment, organizations are opening themselves up to additional cyber threats. Malware attacks are a common threat to cloud security, with studies showing that nearly 90% of organizations [9].

3. Phishing Attacks:

Description: Deceptive attempts to trick individuals into revealing sensitive information, such as login credentials or financial details, often through fraudulent emails or websites [10].

4. Denial of Service (DoS) Attacks:

Description: Overloading a system, network, or service with excessive traffic to make it unavailable for its intended users.

Impact: Disruption of services, downtime.[11]

5. Insider Threats:

Description: Malicious or unintentional actions.

It's important to note that cybersecurity risks can vary based on the specific industry, organization, and the evolving nature of cyber threats. [12]

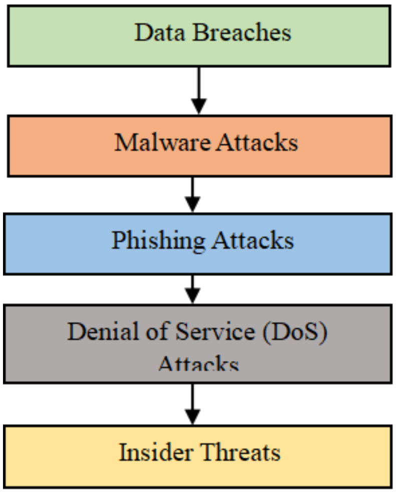


Fig.1.variou risks in cyber security

III. PROPOSED WORK

We propose the following security methods to prevent threats on cyber security.

1) Security Awareness Training:

Educating users about cybersecurity best practices is crucial. Users should be aware of phishing threats, social engineering attacks, and other common tactics used by cybercriminals.

2) Incident Response Plan:

Establishing an incident response plan helps organizations respond effectively to security incidents. This plan outlines the steps to be taken when a security breach occurs, minimizing damage and downtime.

4) Backup and Recovery:

Regularly backing up critical data ensures that organizations can recover information in case of data loss or a ransomware attack. It is important to store backups in a secure and separate location.

5) Network Segmentation:

Dividing a network into segments or zones helps contain security breaches and limit the impact of an attack. It also makes it more challenging for attackers to move laterally within a network.

6) Security Audits and Assessments:

Backup and Recovery Incident Response Plan Regularly assessing and auditing the security posture of an organization's systems and networks helps identify vulnerabilities and weaknesses. This proactive approach allows for timely rem edition.

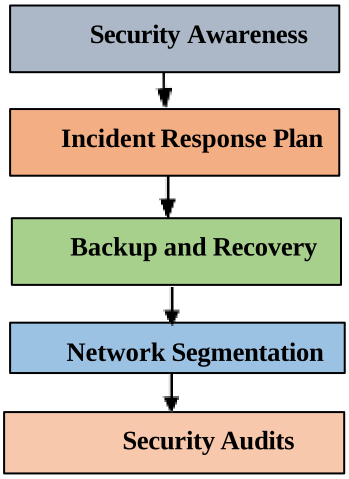
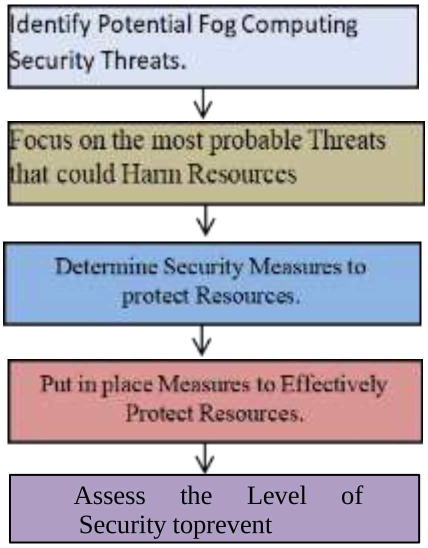


Fig. 2. Measures on cyber security

Algorithm:

1. Begin
2. Identify potential block chain threats
3. Focus on the most probable threats that could
4. Determine security measures to protect
5. Put in place measures to effectively protect.
6. Assess the level of security to prevent.
7. End


Identify Potential Fog Computing Security Threats.
Focus on the most probable Threats that could Harm Resources
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security toprevent

IV. RESULT & ANALYSIS

S. NO	Type of Attacks possible on Cyber Security before implementing the security Measures	Percentage of Vulnerability
1.	Data Breaches	17
2.	Malware Attacks	18
3.	Phishing Attacks	20
4.	Denial of Service (DoS) Attacks	30
5.	Insider Threats	15
Vulnerability before the implementation of proposed Security Measures		100

Table.1. Type of Attacks possible on Cyber Security before implementing the security Measures

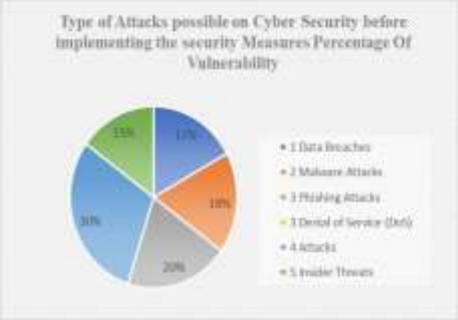


Fig.1. Risk before implementation of Security

S. NO	Type of Attacks possible on Cyber Security after implementing the security Measures	Percentage Of Vulnerability
1.	Data Breaches	10
2.	Malware Attacks	6
3.	Phishing Attacks	5
4.	Denial of Service (DoS) Attacks	2
5.	Insider Threats	7
Vulnerability after the implementation of proposed Security Measures		30

Table.1. Type of Attacks possible on Cyber Security after implementing the security Measures

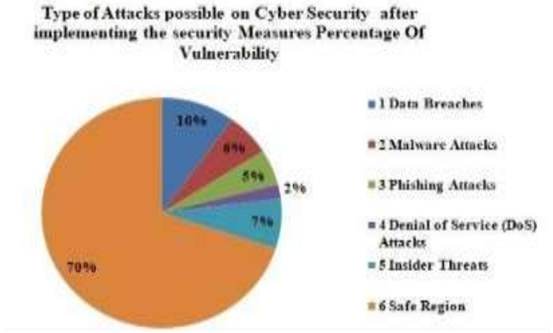


Fig.2. Risks after implementing of Security Measures

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of cyber security. Hackers/ introduces are continuously making attempts to gain the unauthorized access of cyber security using various attacks. Cyber security devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of cyber security several new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] R.A. Kemmerer, “Cyber security”, 03-10 May 2003, DOI: 10.1109/ICSE.2003.1201257

[2] P. Sampath , “An Analysis of Cyber security Risks and Authentication Systems” , 15-17 March 2023,Electronic ISBN:978-93-80544-47-2

[3] Abdul Razzaq, “Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications”, 06-08 March 2013, DOI: 10.1109/ISADS.2013.6513420, Electronic ISBN:978-1-4673-5070-9

[4] Mohit Jain, “Cyber security: Current threats, challenges”, and prevention methods, 10-11 November2022, DOI: 10.1109/ICACCM56405.202 2.10009154, Electronic ISBN:978-1-6654-7439-9

[5] Peter Katsumata, “Cybersecurity risk management”, 31 October 2010 - 03 November 2010, DOI: 10.1109/MILCOM.2010.5680181, Electronic ISSN: 2155-7586

[6] Georgi Tsochev , “Cyber security: Threats and Challenges”07January2021,DOI: 10.1109/ICAI505 93.2020.9311369 , Electronic ISBN:978-1-7281-9308-3

[7] Hajar Barrak Alharbi , “Cyber Risk in Internet of Things World” , 19-21 March 2020 , DOI: 10.1109/ICCAIS48893.2020.9096720 ,Electronic ISBN:978-1-7281-4213-5

[8] Vishal Gupta , “A Systematic review on Cybersecurity: Models, Threats and Solutions” , 29-30April2022,DOI: 10.1109/ICETET-SIP-2254415.2022.9791666 , Electronic ISSN: 2157-0485

[9] Himanshu Arora Cyber Security Challenges and Trends on Recent Technologies, Date of Conference: 29-31 March 2022 DOI: 10.1109/ICCMC53470.2022.9753967

[10] Georgi Tsochev Cyber security: Threats and Challenges, Date of Conference: 01-03 October 2020, Electronic ISBN: 978-1-7281-9308-3, DOI:10.1109/ICAI50593.2020.9311369

[11] Akanksha Verma Cyber Security in Digital SectorDate of Conference: 25-27 March 2021 Electronic ISBN:978-1-7281-9537-7, DOI: 10.1109/ICAIS50930.2021.9395933.

[12] Kamran Shaukat A Survey on Machine Learning Techniques for Cyber Security in the Last Decade Date of Publication: 02 December 2020 Electronic ISSN: 2169-3536 DOI: 10.1109/ACCESS.2020.3041951.

Unleashing Creativity : Exploring the Generative AI

J.Swarna Latha
23CSC08, Student, M.Sc. (Computer Science)
Dept. of Computer Science
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India
swarnalathajujjuvarapu8@gmail.com

P.Saniya
23CSC14, Student, M.Sc. (Computer Science)
Dept. of Computer Science
P.B. Siddhartha College of Arts & Science,
Vijayawada, A.P, India
saniyatahaseen9800@gmail.com

Dr.R.Srinivasa Rao
Associate Professor
Dept. of Business Administration,
P.B.Siddhartha College of Arts & Science, Vijayawada, AP, India.
rsrinirao25@gmail.com

ABSTRACT: Generative AI, A Subset of Artificial Intelligence, Focuses on Creating Systems Capable of Producing Content Autonomously. Leveraging Advanced Algorithms, Such as Generative Adversarial Networks (Gans) And Recurrent Neural Networks, Generative AI Exhibits the Ability to Generate Diverse Outputs, Ranging from Text and Images to Music. This Abstract Explores the Evolution, Applications, And Ethical Considerations Surrounding Generative AI, Highlighting Its Impact on Various Industries and Emphasizing the Need for Responsible Development to Navigate Potential Challenges.

KEYWORDS: Generative Adversarial Networks (Gans), Image Generation, Creative Content Generation, Ethical Considerations, Deep Learning.

I. INTRODUCTION

Artificial Intelligence (AI) refers to the development of computer systems that can perform tasks that typically require human intelligence. This includes learning from experience (machine learning), problem-solving, natural language understanding, and perception. Artificial Intelligence (AI) has grown dramatically and becomes more and more institutionalized in the 21st Century. In this era of interdisciplinary science, of computer science, cybernetics, automation, mathematical logic, and linguistics [1].

Fig.1. Illustration of Generative AI.

The application of AI has brought about efficiency improvement and cost reduction, which are beneficial for economic growth, social development, and human well-being [2]. Generative adversarial networks (GANs) are the most prevalent GAI technique being used today. These systems have been used by companies such as Netflix, Amazon, and YouTube, where they generate personalized playlists, product suggestions, and video recommendations [4]. Creating AGI is a primary goal of some artificial intelligence research and of companies such as Open AI, [5] DeepMind, and Anthropic. AGI is a common topic in science fiction and futures studies. The recent advances in artificial intelligence (AI) can well overcome these challenges, thus spurring an increasing number of organizations and individuals to equip blockchain with AI, making blockchain become more intelligent. However, AI behaviours need to be supervised for ex-post forensics in case of dispute and accountability [6]. Haskell is a very good language for AI. Lazy evaluation and the list and Logic monads make it easy to express non-deterministic algorithms, which is often the case. Infinite data structures are great for search trees. The language's features enable a compositional way to express algorithms. The only drawback is that working with graphs is a bit harder at first because of functional purity. Wolfram Language includes a wide range of integrated machine learning capabilities, from highly automated functions like Predict and Classify to functions based on specific methods and diagnostics. The functions work on many types of data, including numerical, categorical, time series, textual, and image [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in generative ai:

Risks in Generative ai:

1. Privacy:

Privacy concerns can lead to a loss of trust from customers and damage a company's reputation. Generative AI can also be used to generate malicious content, such as disinformation, deep fakes, and hate speech [8].

2. Legal problems:

Suppose the content generated by the AI is inaccurate, inaccessible, or offensive. In that case, legal action may be taken against the creators or users of the technology, leading to significant financial and reputational damage [9]**.**

3. Financial issues:

If the content generated by the AI is not accurate, accessible, or appropriate for the intended audience, it could result in lost revenue or other financial consequences. This could be particularly problematic for companies [10].

4. Ethical non-compliance:

If the content generated by the AI perpetuates harmful stereotypes or promotes misinformation, it could have real-world consequences for individuals or groups, leading to ethical non-compliance and damage to the company's reputation [11].

5. Poor performance:

Imagine that the critical business systems rely on malfunctioning AI API - this will cause critical processes to be slowed down or stopped, which will endanger the results [12].

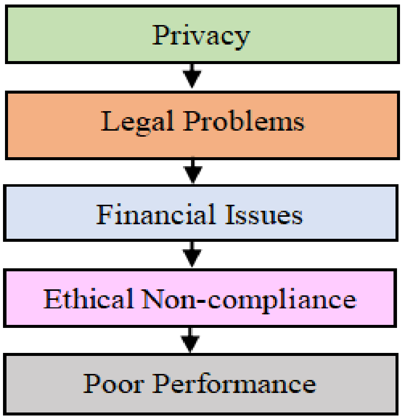


Fig. 1. Various Risks of Generative AI

III. PROPOSED WORK

We propose the following security methods to prevent threats on generative ai:

1. **Perplexity:** Measures how well the model predicts a sample. Lower perplexity indicates better performance**.**
2. **BLEU Score:** Evaluates the quality of machine-generated text by it to reference texts. Higher BLEU scores suggest better.
3. **Inception Score**: Evaluates the quality and diversity of generated images. Higher scores indicate better performance.
4. **Success Rate:** Measures the percentage of generated samples that meet specific criteria, indicating the model's success in achieving a desired outcome**.**
5. **ROUGE Score:** Assesses the similarity between machine-generated and reference texts, commonly used in text.

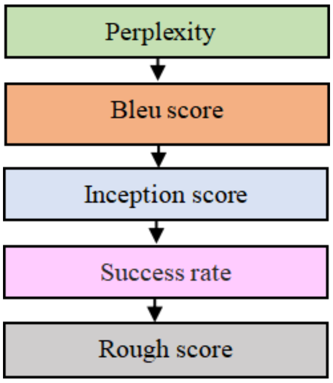


Fig.2.Various measures to generative AI

Algorithm:

1. Begin
2. Identify potential ai security Threats.
3. Focus on the most probable threats that could. Determine security measures to protect resources.
4. Put in place measures to effectively protect resources.
5. Asses the level of security to prevent authorized.
6. End.

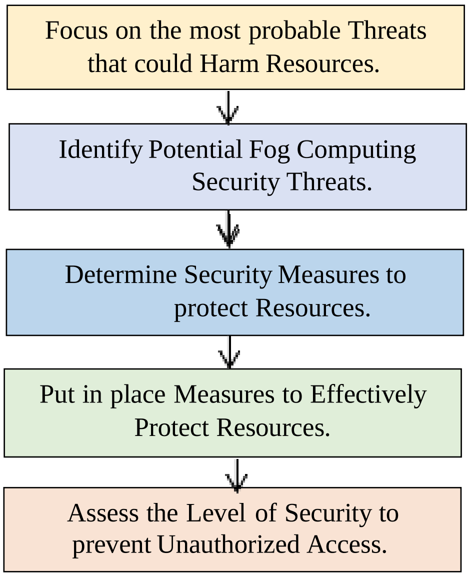

Focus on the most probable Threats that could Harm Resources.
Identify Potential Fog Computing Security Threats.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 3. Procedure to safeguard the resources of generative AI

IV. RESULT & ANALYSIS

S. No	Types of attacks possible on Generative AI before implementingthe Security Risks	Percentage of Vulnerability
1	Privacy	19
2	Legal problems	23
3	Financial issues	19
4	Ethical non-compliance	18
5	Poor performance	21
Vulnerability before the implementation ofproposed Security Risks		100

Table 1. Types of Possible Attacks on Generative AI before implementing the Security Risks

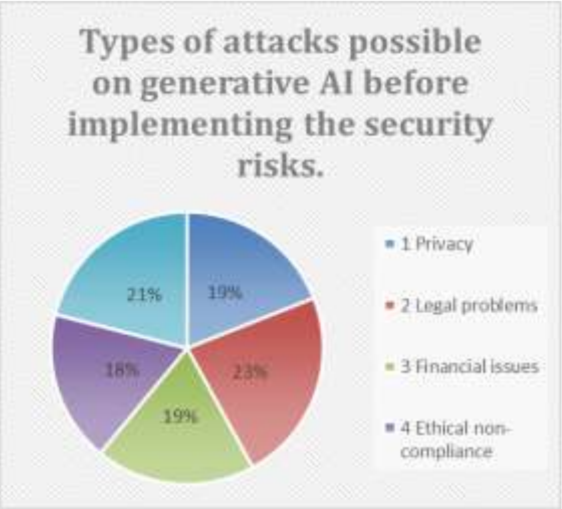


Fig.4.Risk before implementation of Security Measures.

S. No	Types of attacks possible on Fog Computing after implementing the Security measures	Percentageof Vulnerability
1	Privacy	7
2	Legal problems	5
3	Financial issues	7
4	Ethical non-compliance	5
5	Poor performance	6
Vulnerability after the implementation of proposed Security Measures		30

Table 2. Types of Possible Attacks on Fog Computing after implementing the Security Measures

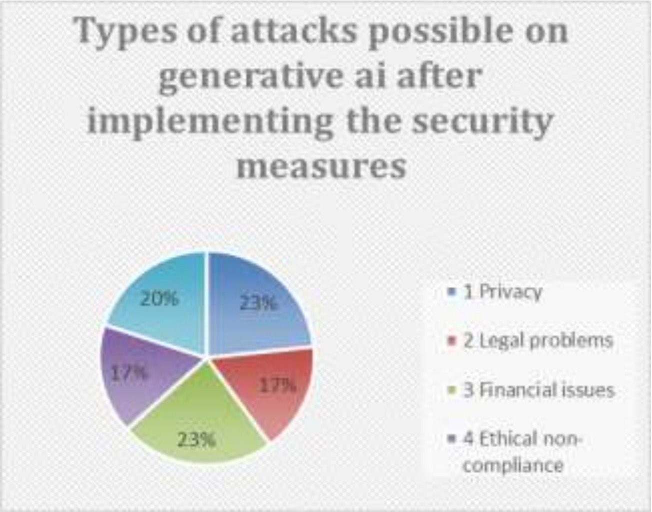


Fig.5. Risk after implementation of Security Measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of generative AI. Hackers/ introduces are continuously making attempts to gain the unauthorized access of generative ai using various attacks. Generative ai devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of generative ai several new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Jiaying Liu, Artificial Intelligence in the 21st Century Date of Publication: 26 March 2018Electronic ISSN: 2169-3536, DOI: 10.1109/ACCESS.2018.2819688.

[2] Changwon HuangAn Overview of Artificial Intelligence EthicsDate of Publication: 28 July 2022, Electronic ISSN: 2691-4581 DOI: 10.1109/TAI.2022.3194503

[3] Mlađan JovanovićGenerative Artificial Intelligence: Trends and Prospects Date of Publication: 27 September 2022 Electronic ISSN: 1558-0814, DOI:10.1109/MC.2022.3192720

[4] Baran, Remigiu(1 June 2018). "A capable multimedia content discovery platform based on visual content analysis and intelligent data enrichment". doi:10.1007/s11042-017-5014-1. ISSN 1573-7721. S2CID 36511631.

[5] Shevlin, (4 October 2019). "The limits of machine intelligence: Despite progress in machine intelligence, artificial general intelligence is still a major challenge". doi:10.15252/embr.201949177. ISSN 1469-221X

[6] Yushu ZhangRecording Behaviors of Artificial Intelligence in Blockchains Date of Publication: 11 October 2022
Electronic ISSN: 2691-4581 DOI: 10.1109/TAI.2022.3213531
[7] Hua ZhangArchitectures and Use cases of AI-based NetworkDate of Conference: 15-18 October 2021 Electronic ISBN:978-1-6654-3188-0
DOI: 10.1109/ICAIT52638.2021.9701988
[8] Mohammad Ali Al Qudrah Using Artificial Intelligence Applications For E-Government Services As Iris Recognition Date of Conference: 18-20 October 2023 Electronic ISBN:979-8-3503-0356-8
DOI: 10.1109/AICT59525.2023.10313183
[9] Samuel LefcourtAI Forensics Date of Conference: 06-08 June 2023 Electronic ISBN:979-8-3503-2601-7 DOI: 10.1109/ICAA58325.2023.00023, Publisher: IEEE
[10] Virgílio Almeida On the Development of AI Governance Frameworks Date of Publication: 14 February 2023 Electronic ISSN: 1941-0131, DOI: 10.1109/MIC.2022.3186030
[11] Jude Osakwe Artificial Intelligence: A Veritable Tool for Governance in Developing Countries Date of Conference: 23-25 November 2021 Electronic ISBN:978-1-6654-1749-5
DOI: 10.1109/IMITEC52926.2021.9714584
[12] Pascual Review of the Use of AI Techniques in Serious Games: Decision Making and Machine learning
Date of Publication: 25 December 2015 Electronic ISSN: 1943-0698, DOI: 10.1109/TCIAIG.2015.2512592.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Navigating Risks in the Era of Artificial Intelligence

K.KISHORE
23CSC09, Student, M.Sc.(computer science)
Dept. of computer Science
P.B.Siddhartha College of Art & Science
Vijayawada, A.P, India
kishork1026@gmail.com

G.RADHA KRISHNA
23CSC23, Student, M.Sc.(computer science)
Dept. of computer Science,
P.B.Siddhartha College of Art & Science
Vijayawada, A.P, India
sairadhakrishna1115@gmail.com

CH.NITHIN
23CSC20, Student, M.Sc.(computer science)
Dept. of computer Science,
P.B.Siddhartha College of Art & Science
Vijayawada, A.P, India
chigurupatinithin18@gmail.com

ABSTRACT: This Research Delves into The Intricate Web of Risks Accompanying the Proliferation of Artificial Intelligence (AI) Across Diverse Domains Combining A Systematic Literature Review, Case Studies, And Expert Insights, The Study Scrutinizes Technical Risks, Encompassing Issues Like Algorithmic Bias, System Reliability, And Vulnerability to Adversarial Attacks. Ethical Dimensions Are Explored, Shedding Light on Transparency, Accountability, And Societal Impacts, Including Concerns About Bias and Discrimination. By Offering A Concise Analysis of These Risks, The Article Provides Actionable Insights for Policymakers, Practitioners, And Researchers. The Study Emphasizes the Necessity for Robust Governance, Ethical Guidelines, And Technical Safeguards to Ensure the Responsible Development Of AI Technologies In Our Interconnected World.

KEYWORDS: Artificial Intelligence (AI), Risks, Systematic Literature Review, Case Studies, Expert Insights, Algorithmic Bias.

I. INTRODUCTION

Artificial intelligence (AI) methods are mainly used to solve highly complex tasks, such as processing natural language or classifying objects in images. AI methods do not only allow significantly higher levels of automation to be achieved, but they also open up completely new fields of application [1]. The importance of artificial intelligence is constantly increasing due to ongoing research successes and the introduction of new applications based on this technology. Driven by success in the fields of image recognition, natural language processing and self-driving vehicles, in the coming years, the fast-growing market of artificial intelligence (AI) will play an increasingly significant role in occupational safety [2,3]. Today, the term artificial intelligence is mainly used in the context of machine learning, such as decision trees or support vector machines, but also includes a variety of other applications, such as expert systems or knowledge graphs [4]. A significant subcategory of machine learning is deep learning, which deals with the development and application of deep neural networks. These neural networks are optimised and trained for specific tasks, and they can differ fundamentally in terms of their architecture and mode of operation [5]. An example would be the use of convolutional neural networks in the field of image processing [6]. AI systems are engineered systems that build, maintain, and use a knowledge model to conduct a predefined set of tasks for which no algorithmic process is provided to the system. Thus, by using artificial intelligence, concepts such as learning, planning, perceiving, communicating and cooperating can be applied to technical systems. These capabilities enable entirely new smart systems and applications, which is why artificial intelligence is often seen as the key technology of the future [7]. Protective devices and control systems based on artificial intelligence have already enabled fully automated vehicles and robots to be created [8,9]. Furthermore, they enable accidents to be prevented by assistance systems capable of recognising hazardous situations [10].

II. RELATED WORK

Several risks in Artificial Intelligence (AI): Artificial Intelligence (AI) presents various opportunities and benefits, but it also comes with several risks and challenges. Some of the key risks associated with AI include:

i. **Ethical Considerations:**
1. Ethical dilemmas may arise in various AI applications, such as autonomous weapons, surveillance systems, or decision- making in sensitive areas like healthcare.
2. Establishing ethical guidelines and frameworks for AI development and deployment is crucial.

ii. **Privacy Issues:**
1. AI systems often require vast amounts of data for training, and the handling of personal data raises concerns about privacy.
2. Unauthorized access to sensitive information or the misuse of AI-generated insights can compromise individual privacy.

iii. **Regulatory Challenges:**
1. The rapid evolution of AI technology can outpace regulatory frameworks, making it difficult for governments to establish and enforce appropriate regulations.

2. Striking a balance between fostering innovation and ensuring responsible AI use is an ongoing challenge.

iv. Reliability and Accountability:

1. AI systems may exhibit unexpected behavior or fail in certain situations, raising concerns about their reliability.
2. Determining responsibility and accountability when AI systems make errors or because harm can be challenging.

v. Exacerbating Inequality:

1. Access to and benefits from AI technology may not be evenly distributed, potentially exacerbating existing social and economic inequalities.

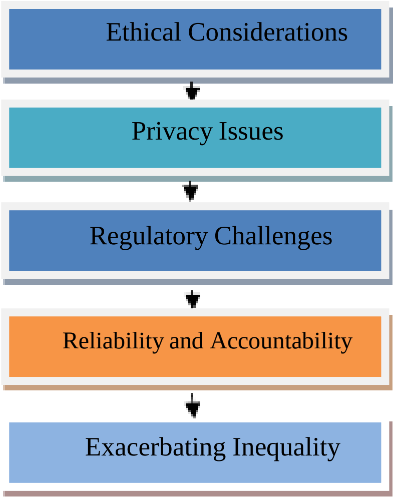


Fig.1.Several risks in Artificial Intelligence (AI)

III. PROPOSED WORK

Securing Artificial Intelligence (AI) systems is crucial to prevent vulnerabilities and potential threats. Here are measures to overcome security challenges in AI:

1) **Data Privacy and Protection should be maintained:** Implement robust data privacy measures, including encryption and anonymization, to protect sensitive information used in training AI models.
2) **Adversarial Training is adopted:** Train AI models with adversarial examples to enhance their resilience against adversarial attacks.
3) **Regular Security Audits should be conducted:** Conduct regular security audits and assessments to identify and address vulnerabilities in AI systems.
4) **Access Control and Authentication is enforced:** Implement strong access controls and authentication mechanisms to restrict unauthorized access to AI systemsand data.
5) **Update and Patching is done regularly:** Keep AI software and frameworks up-to-date with the latest security patches to address known vulnerabilities.

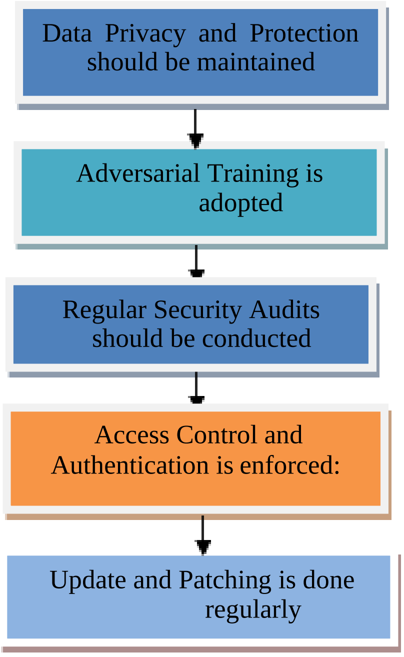

Data Privacy and Protection should be maintained
Adversarial Training is adopted
Regular Security Audits should be conducted
Access Control and Authentication is enforced:
Update and Patching is done regularly

Fig. 2. Various measures to Artificial intelligence

Algorithm:

1. **Define Scope and Objectives:** Clearly outline the purpose and goals of the AI system.
2. **Risk Identification:** Identify potential technical, ethical, legal, and societal risks.
3. **Regulatory Compliance:** Ensure adherence to existing AI regulations and stay updated on emerging standards.
4. **Ethical Assessment:** Evaluate ethical implications, addressing biases, transparency, and accountability.
5. **Transparency and Explain ability:** Implement mechanisms for transparent and explainable AI decision-making.

IV. RESULT &ANALYSIS

S.No	Types of on attacks on AI applications beforeimplementing the security measures	Percentage of vulnerability
1	Ethical Considerations	24
2	Privacy Issues	20
3	Regulatory Challenges	18
4	Reliability and Accountability	19
5	Exacerbating Inequality	19
Vulnerability before the implementation of Proposed security Measurement		100

Table 1. Types of possible Attacks on Artificial Intelligence (AI) before implementing the Security Measures

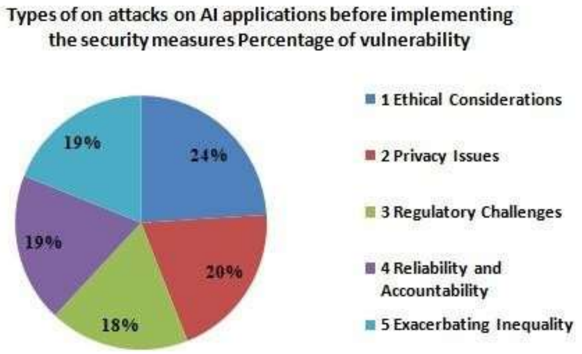


Fig.1. Vulnerability before implementing the Security Measures in Artificial Intelligence

S.No	Types of on attacks on AI applications afterimplementing the security measures	Percentage of vulnerability
1	Ethical Considerations	4
2	Privacy Issues	6
3	Reliability and Accountability	4
4	Reliability and Accountability	6
5	Exacerbating Inequality	6
Vulnerability after the implementation of Proposed security Measurement		26
Table 2. Types of possible Attacks on Artificial Intelligence (AI)after implementing the Security Measures		

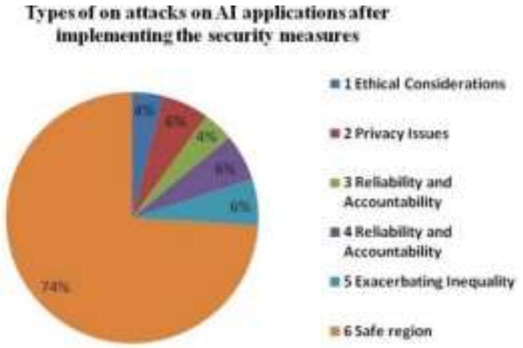


Fig. 2. Enhancement of Security after implementing Security Measures in Artificial Intelligence

After implement the security measures we have restricted most of the security threats from 100 to 26.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of Artificial intelligence devices. Hackers /introduces are continuously making attempt to gain the unauthorized access of Artificial intelligence devices using various attacks, as Artificial intelligence devices has an effect on their usage, in order protect the security and integrity of Artificial intelligence devices several new security measures.

VI. REFERENCES:

[1] Adiani, D., Breen, M., Migovich, M., Wade, J., Hunt, S., Tauseef, M., Khan, N., Colopietro, K., Lanthier, M., Swanson, A., Vogus, T. J., & Sarkar, N. (2023). Multimodal job interview simulator for training of autistic individuals. Assistive Technology, 1–18.

[2] Bakken, S. (2023). AI in health: Keeping the human in the loop. Journal of the American Medical Informatics Association, 30(7), 1225–1226.

[3] Critch, A., & Russell, S. (2023). TASRA: A taxonomy and analysis of societal-scale risks from AI.

[4] Daneshjou, R., Smith, M. P., Sun, M. D., Rotemberg, V., & Zou, J. (2021). Lack of transparency and potential bias in artificial intelligence data sets and algorithms: A scoping review. JAMA Dermatology, 157(11), 1362–
1369.

[5] European Disability Forum. (2023). Resolution on the EU artificial intelligence act for the inclusion of persons with disabilities - European disability forum.

[6] Jaddoh, A., Loizides, F., & Rana, O. (2022). Interaction between people with dysarthria and speech recognition systems: A review. Assistive Technology, 35(4), 330–338.

[7] Kahraman, M., & Turhan, C. (2021). An intelligent indoor guidance and navigation system for the visually impaired. Assistive Technology, 34(4), 478–486.

[8] Kamikubo, R., Wang, L., Marte, C., Mahmood, A., & Kacorri, H. (2022). Data representativeness in accessibility datasets: A meta-analysis. In ASSETS 2022- Proceedings of the 24th International ACM SIGACCESS Conference on Computers and Accessibility.

[9] Khan, M., & Hanna, A. (2022). The subjects and stages of AI dataset development: A framework for dataset accountability. SSRN Electronic Journal.

[10] Kim, S. K., Jang, J. W., Hwang, Y. S., Lee, O. E. K., & Jo, H. S. (2023). Investigating the effectiveness of socially assistive robot on depression and cognitive functions of community dwelling older adults with cognitive impairments. Assistive Technology, 1–9.

[11] Landuran, A., Sauzéon, H., Consel, C., & N'Kaoua, B. (2022). Evaluation of a smart home platform for adults with down syndrome. Assistive Technology, 35(4), 347– 357.

Comprehensive Measures to Counteract Risks in Edge Computing

N.P.B.Siva Naga Mani
23CSC29, Student, M.Sc.(computer science)
P.B. Siddhartha College of Arts &Science
Vijayawada, AP, India
sivanagamaninunna@gmail.com

K.Hepsiba
23CSC10, Student, M.SC.(computer science)
P.B. Siddhartha college of Arts& Science
Vijayawada, AP, India
kolusuhepsiba@gmail.com

G. Prathyusha,
23CSC05, Student, M.SC.(computer science)
P.B. Siddhartha College of Arts& Science
Vijayawada, AP, India
Prathyushagovada7@gmail.com

ABSTRACT: Edge Computing Is A Distributed Computing Paradigm That Brings Data Storage and Computation Closer to Data Sources. Edge Computing Is A Topology- And Location- Sensitive Form of Distributed Computing; The Term Refers to Architecture Rather Than A Specific Technology. It Was Created in The Late 1990s To Serve Video and Web Content, Its Origin Lies in Content Delivery Networks. In the Early 2000s, These Networks Evolved to Host. Edge Computing Is A Distributed Computing Paradigm That Brings Data Storage and Computation Closer to Data Sources. Edge Computing Is A Topology- And Location- Sensitive Form of Distributed Computing; The Term Refers to Architecture Rather Than A Specific Technology. It Was Created in The Late 1990s To Serve Video and Web Content, Its Origin Lies in Content Delivery Networks. In the Early 2000s, These Networks Evolved to Host Applications and Application Components at The Edge Servers,[5] Resulting in The First Commercial Edge Computing Services That Hosted Applications Such as Dealer Locators, Shopping Carts, Real-Time Data Aggregators, And Ad Insertion Engines.

KEYWORDS: Evolution, Streaming, Real, Resource, Task, Edge, Smart, Computing, Internet, Mobile, Remote, Container.

I. INTRODUCTION

The Internet of Things (IoT) is playing a major role across a variety of vertical sectors by generating tremendous cost savings and new revenue streams. As a result, it is the common consensus that the next- generation wireless networks should efficiently and reliably support massive IoT connectivity with guaranteed quality of service (QoS). Traditionally, the IoT applications are executed in a centralized manner (i.e., via cloud computing), where the tasks of IoT devices are collected at a remote centralized cloud server for further processing [1]. The amount of data generated by devices worldwide has also increased from 218ZB in 2016 to 847 ZB in 2021. International data company Internet Data Center (IDC) statistics show that by 2020, the number of terminals and devices connected to the network will exceed 50 billion, and the total global data in 2020 will also exceed 40 ZB [2]. Security and privacy: For example, when using various applications in smart phones, applications will require user data, including privacy data. There is a high risk of privacy leakage or attack on this data when uploaded to the cloud center. Energy consumption: the number of smart devices continues to increase, and the power consumption of data centers in China has increased significantly. Improving the use efficiency of cloud computing energy consumption [3] cannot meet the increasing demand for data energy consumption. The rapidly developing intelligent society will have higher requirements for the energy consumption of cloud computing. This process creates great pressure on the network, specifically in the data transmission costs of bandwidth and resources. In addition, the performance of the network will worsen with increasing data size. A more critical situation arises for IoT applications that are time-sensitive, meaning that very short response times are non-negotiable (the smart transportation [4] Rodrigo and his team analyzed and surveyed the security threats associated with the various edge computing related paradigms, such as fog computing, and mobile edge computing. However, the survey considered techniques related to authenticity requirement, whereas, less attention was given to other requirements. Guan et al [5]. More in general at the edge of any network. The basic idea behind MEC is that by running applications and performing related processing tasks closer to the cellular customer, network congestion is reduced and applications perform better. MEC technology is designed to be implemented at the cellular base stations or other edge nodes, and enables flexible and rapid deployment of new applications and services for customers. Combining elements of information technology and telecommunications networking, MEC also allows cellular operators to open their radio access network (RAN) to authorized third parties, such as application developers and content providers [6]. Edge detection includes a variety of mathematical methods that aim at identifying edges, defined curves in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The same problem of finding discontinuities in one- dimensional signals is known as step detection and the problem of finding signal discontinuities over time is known as change detection. Edge detection is a fundamental tool in image processing, machine vision and computer vision, particularly in the areas of feature detection and feature extraction [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in edge computing:

RISKS IN EDGE COMPUTING:

1) Edge Security Risks

Edge computing involves a distributed system, and any distributed system has a broad attack surface -a larger number of devices need to be secured. Each individual Internet of Things (IOT) device could be vulnerable and potentially render the entire network vulnerable.

2) Computing Burden

If the data demands extremely high processing volumes, the burden may need to be shifted from the edge to the cloud. As an example, most "voice analysis" systems today (such as transcription services) will send voice snippets to a cloud server to be analysed, as the device itself may not have the processing power - so the edge isn't a good use case for these.

3) Hardware Security

If the hardware involved is vulnerable, edge computing becomes a substantially higher risk. Edge computing for high-security data is generally completed on close proximity servers or devices rather than on an end-user device - for example, authentication for kiosk tablets within a financial institution would occur on the company's local authentication servers or WAN rather than on an individual's tablet or the cloud.

4) Security Best Practices

In practice, edge security is simple: know who you are dealing with (authentication) and provide authenticated users with the least possible potential for damage (least privilege). To keep your systems secure, you'll need to follow a few best practices.

5) Automated &Intelligent Monitoring

Edge computing systems can become large and unwieldy. Automated, intelligent monitoring systems increase the chances of detecting security risks without demanding the attention of a human operator. Imagine a warehouse that has thousands upon thousands of sensors. An artificial intelligence-driven security system would validate that these sensors are fully patched, secured, and operating as they should.

III. PROPOSED WORK

We proposed the following security methods of safeguard with Edge Computing from varioussecurity attacks.

Measures to Overcome Risks on Edge Computing:

1. Improved Connectivity

Enhance network infrastructure to ensure seamless connectivity between edge devices and the central cloud. Utilize technologies like 5G, mesh networking, or edge-specific protocols to reduce latency and ensure reliable connections.

2. Data Security

Implement robust security measures to protect data at the edge. This includes encryption, access control, regular updates, and security patches to safeguard against potential vulnerabilities.

3. Device Management

Employ effective device management solutions to monitor, update, and manage edge devices remotely. This ensures efficient performance and enables quick troubleshooting.

4. Optimized Workloads

Distribute workloads effectively across edge devices and the cloud to balance processing power and reduce latency. Employ edge analytics to process data locally and transmit only necessary information to the cloud.

5. Regulatory Compliance

Ensure compliance with relevant data privacy and regulatory requirements, especially when dealing with sensitive data at the edge.

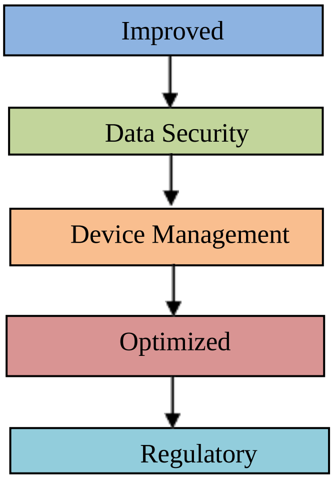


Fig. 1 Various Measures to overcome risks on edge computing

Algorithm:

1. Begin
2. Identify potential Computing Security Threats.
3. Focus on the most probable Threats that could HarmResource.
4. Determine Security Measurement to Protect Resource.
5. Put in place Measures to Effectively Protect Resources.
6. Asses the level of security to prevent UnauthorizedAccess.
7. End.

IV. RESULT AND ANALYSIS

S. No	Types of Attacks possible on Edge computing Technology before implementing the security measures	Percentage of vulnerability
1	Edge security risks	35
2	Computing burden	9
3	Hardware security	28
4	Edge security best practices	15
5	Automated & intelligent monitoring	13
Vulnerability before the Implementation of proposedsecurity Measures		100
Table 1. Types of possible Attacks on Edge computing Technology before implementing the security measures.		

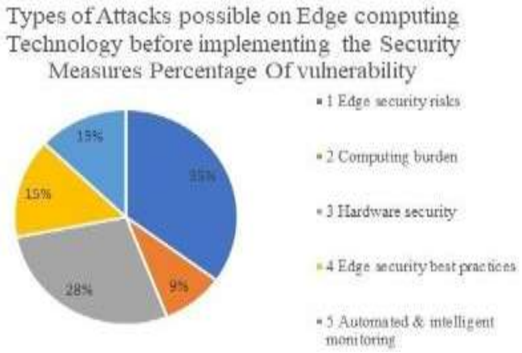


Fig.2 Risks before implementation of security measures

S. No	Types of Attacks possible on Edge computing Technology after implementing the security measures	Percentage Of vulnerability
1	Improved Connectivity	
2	Data Security	6
3	Device Management	5
4	Optimized Workloads	5
5	Regulatory Compliance	6
Vulnerability after the Implementation of proposedsecurity Measures		30
Table 2. Types of possible Attacks on Edge computing Technology after implementing the security measures.		

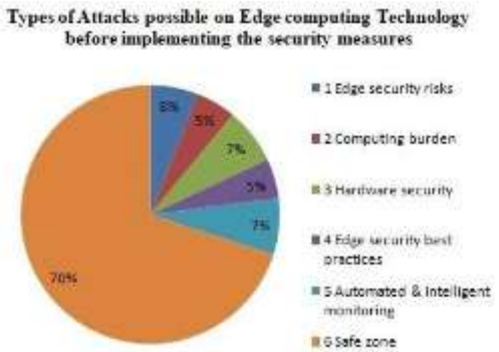


Fig.3. Risks after implementation of security Measures of edge computing

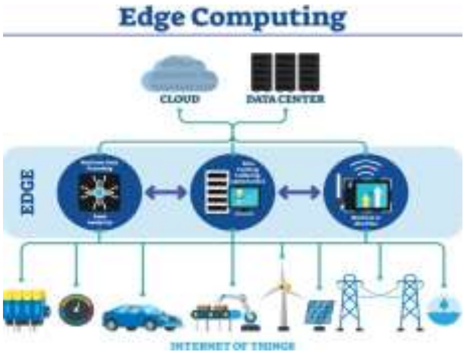
V. FUTURE WORK

The future of edge computing in your industry:

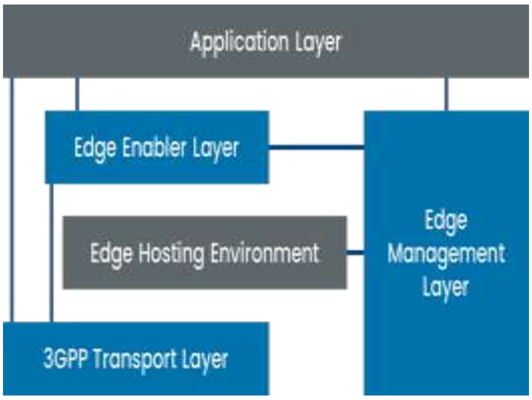
CIOs in banking, mining, retail, or just about any other industry, are building strategies designed to personalize customer experiences, generate faster insights and actions, and maintain continuous operations. This can be achieved by adopting a massively decentralized computing architecture, otherwise known as edge computing. Within each industry, however, are particular uses cases that drive the need for edge IT. Banks may need edge to analyze ATM video feeds in real-time in order to increase consumer safety. Mining companies can use their data to optimize their operations, improve worker safety, reduce energy consumption and increase productivity. Retailers can personalize the shopping experiences for their customers and rapidly communicate specialized offers. Companies that leverage kiosk services can automate the remote distribution and management of their kiosk- based applications, helping to ensure they continue to operate even when they aren't connected or have poor network connectivity.

Real-Life Use Cases for Edge Computing:

Depending on how many of the 30 billion Internets of Things (IoT) devices forecast for global deployment by 2020 rely on the cloud, managing the deluge of IoT generated data makes proper processing seem near impossible. Traditional cloud computing has serious disadvantages, including data security threats, performance issues, and growing operational costs. Because most data saved in the cloud has little significance and is rarely used, it becomes a waste of resources and storage space.



Edge enabler layer: The edge enabler layer provides Application Programming Interfaces (APIs) for the application developers to leverage edge capabilities. With this layer, the application developers are able to locate, connect, and switch to the most suitable application server on the edge network, and to exploit the potential of the underlying 3GPP network in optimizing the service.



VI. CONCLUSION

Edge computing is the new computing paradigm, as cloud computing alone cannot sufficiently support the needs of industrial enterprises on the path to smart manufacturing. This challenge is primarily due to constraints around bandwidth, latency, security, and privacy concerns associated with processing large amounts of data, including sensitive data and information. Edge computing is paving the way for new applications and services to exist closer to the user and data sources in a processing or manufacturing facility. As this new paradigm is adopted at scale by enterprises for their numerous facilities, it becomes a daunting challenge for the IT workforce to manage the proliferation of diverse applications, compute and network infrastructures, and support services across the facilities. The OT workforce may see a diminishing value of IT in support of their technologies on their factory floor or shop floor. Siloed deployments can lead to redundancy of applications and services across facilities. This redundancy creates overhead cost for enterprise leadership to manage and support, while ensuring that enterprise objectives around digital transformation and smart manufacturing are met. Enterprise IT must consider adopting a IEMapproach to manage edge compute infrastructure aseach facility embraces the edge to deploy new use cases with enabling and emerging technologies across their facilities. This document has introduced the concept and importance of IEM for industrial enterprises. It highlights the alignment gap and outlines a model design balancing the enterprise leadership vision of smart manufacturing and the constraints of individual facilities. Model design sets up a foundation for the IEM of an enterprise and the execution of edge computing through reviewing of current facility IT capabilities to support OT. This document also provided a reference capability model to review the readiness of every facility, as well as a robust list of edge enabling use cases. Finally, the document introduced Dell Technologies as an enabler of IEM and attempts to simplify the edge for the industrial sector on their digital transformation journey.

VII. REFERNECE:

[1] Malong Ke, An Edge Computing Paradigm for Massive IoT Connectivity Over High-Altitude Platform Networks October 2021, DOI: 10.1109/MWC.221.2100092, Electronic ISSN: 1558-0687

[2] V. Turner, J. F. Gantz and D. Reinsel, The digital universe of opportunities: Rich Data and the Increasing Value of the Internet of Things, Nov. 2018, [online] Available: https://www.emc.com/leadership/digitaluniv erse/2014iview/index.htm.
Show in Context Google Scholar

[3] Y. Q. Gao, H. Bguan and Z. W. Qi, "Service level agreement based energy-Effificient resource man agreement in cloud data centers", Compute. Elect. Eng., vol. 40, pp. 1621-1633, 2014.

[4] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu and W. Zhao, "A real-time en-route route guidance decision scheme for transportation-based cyber physical systems", IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2551-2566, Mar. 2017.

[5] Z. Guan, Y. Zhang, G. Si, Z. Zhou, J. Wu, S. Mumtaz, et al., "ECOSECURITY: Tackling challenges related to data exchange and security: An edge-computing-enabled secure and efficient data exchange architecture for the energy Internet", IEEE Consum. Electron. Mag., vol. 8, pp. 61-65, Mar. 2019

[6] "Mobile Edge Computing Introductory Technical White Paper" (PDF). etsi.org. 2014-09-01.
Retrieved 2015-10-26

[7] Umbaugh, Scott E (2010). Digital image processing and analysis: human and computer vision applications with CVIPtools (2nd ed.). Boca Raton, FL: CRC Press. ISBN 978-1-4398-0205-2.

[8] Abdulmalik Alwarafy, A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things, 10 August 2020,
DOI: 10.1109/JIOT.2020.3015432, Electronic ISSN: 2327-4662

[9] Isabela Miranda de Mendonça, Reduction of the Computational Burden of the TEP Problem by a Minimum-Effort Heuristic Algorithm, 28 June 2021 - 02 July 20.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Foggy Horizons : Exploring the Risks and Safeguarding Strategies in Fog Computing

K.KRISHNA PRASANNA
23CSC11, Student, M.Sc.(Computer Science)
Dept. of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
prasannakona2001@gmail.com

A.SAI TEJASWI
23CSC18, Student, M.SC.(Computer science)
Dept. of Computer science
P.B.Siddhartha college of Arts & Science
Vijiyawada,AP,India
saitejaswiavanigadda@gmail.com

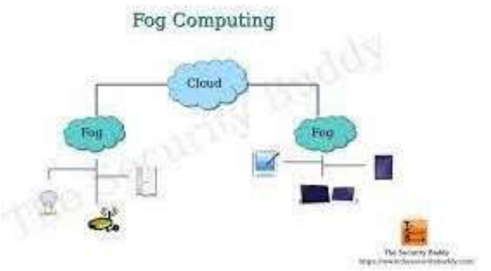
Y.PADMAJA
23CSC16, Student, M.Sc.(Computer Science)
Dept. of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India.
padmajayamanda4015@gmail.com

ABSTRACT: Fog Computing Is A Way of Doing Computing That Brings Data Storage and Processing Closer to Where It's Needed Rather Than Relying on Distant Cloud Servers. Think of It Like This: If Cloud Computing Is Like Storing and Processing Everything in A Big, Far-Away Data Center, Fog Computing Is About Doing Some of That Work Closer to Your Home or Device. In Fog Computing, Smaller, Localized Data Centers or Devices Called Fog Are Placed at Various Points in A Network, Closer to Where Data Is Created or Used. These Nodes Can Be Anything from Routers and Switches to Iot Devices or Even Smart Appliances. By Doing Some Processing and Storing Data Closer

KEYWORDS: Malicious, Access Control, Network, Security, Authentication.

I. INTRODUCTION

Fog computing is a distributed computing paradigm that acts as an intermediate layer in between Cloud data centres and IoT devices/sensors. It offers computer, networking and storage facilities so that Cloud-based services can be extended closer to the IoT devices/sensors [1]. The concept of Fog computing was first introduced by Cisco in 2012 to address the challenges of IoT applications in conventional Cloud computing. IoT devices/sensors are highly distributed at the edge of the network along with real-time and latency-sensitive service requirements. Since Cloud data centres are geographically centralized, they often fail to deal with storage and processing demands of billions of geo- distributed IoT devices/sensors. As a result, congested network, high latency in service delivery, poor Quality of Service (QoS) are experienced [2]. Typically, a Fog computing environment is composed of traditional networking components e.g. routers, switches, set top boxes, proxy servers, Base Stations (BS), etc. and can be placed at the closer proximity of IoT devices/sensor. These components are provided with diverse computing, storage, networking, etc. capabilities and can support service-applications execution.



Consequently, the networking components enable Fog computing to create large geographical distributions of Cloud-based services. Besides, Fog computing facilitates location awareness, mobility support, real-time interactions, scalability and interoperability [3]. Thereby, Fog computing can perform efficiently in terms of service latency, power consumption, network traffic, capital and operational expenses, content distribution, etc. In this sense, Fog computing better meets the requirements with respect to IoT applications compared to a solely use of Cloud computing [4]. However, the concept of Fog computing is very much similar to the existing computing paradigms [5]. In this chapter, we elaborately discuss the fundamental differences of Fog computing with other computing paradigms. Here, we also analyse different aspects of Fog computing including corresponding resource architecture, service quality, security issues, etc. and review recent research works from the literature. We present a taxonomy based on the key properties and associated challenges in Fog computing [6].

II. RELATED WORK

In this section, we exemplify various Security Risks in Fog Computing:

Risks in Fog Computing:

1. **Advance Persistent Threats (APT):** Advance Persistent Threats are cyber-attacks whereby the aim is to compromise a company's infrastructure with the desire to steal data and intellectual property [7].
2. **Access Control Issues (ACI):** Access Control Issue can result in poor management and any unauthorized user being able to acquire data and permissions to install software and change configurations [8].
3. **Account Hijacking (AH):** Account Hijacking is where an attack aims to hijack the user accounts for malicious

purpose. Phishing is a potential technique for account hijacking [9].

4. **Denial of Service (DOS):** Denials of services are where legitimate users are prevented from using a system (data and applications) by overwhelming a system's finite resources [10].
5. **Data Breaches (DB):** Data breaches are when sensitive, protected or confidential data is released or stolen by an attacker [11].
6. **Data Loss (DL):** Data loss is where data is accidentally (or maliciously) deleted from the system. This does not have to be resulting from a cyber-attack and can arise through natural disaster [12].

III. PROPOSED WORK

We propose the following security methods to prevent threats on Fog Computing.

1. **Vendor Security Assurance:** When using third-party solutions or devices, conduct thorough security assessments of vendors and their products. Ensure that vendors follow security best practices and provide regular updates and patches.
2. **Incident Response Plan:** Develop and implement an incident response plan to efficiently respond to and recover from security incidents. This plan should include procedures for identifying, isolating, and mitigating security breaches.
3. **Privacy Considerations:** Address privacy concerns by implementing measures to protect sensitive information. This includes the data when necessary and complying with relevant data protection regulations.
4. **Employee Training:** Provide ongoing training for employees and users on security best practices and awareness. Educate them about potential risks and the importance of following security policies and procedures.
5. **Risk Assessment:** Conduct regular risk assessments to identify and evaluate potential security threats. Adjust security measures based on the evolving threat landscape and the specific characteristics of the fog computing.

Algorithm:

```
1.  Begin
2.  Identify Potential Fog Computing Security
    Threats.
3.  Focus on the most probable Threats that
    could HarmResources.
4.  Determine Security Measures to protect
    Resources.
5.  Put in place Measures to Effectively
    Protect Resources.
6.  Assess the Level of Security to prevent
    UnauthorizedAccess.
7.  End
```

IV. RESULT & ANALYSIS

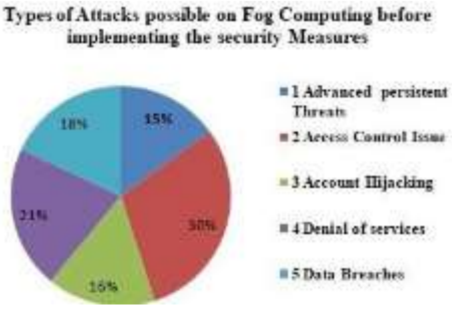


Fig.1. Risk in Fog Computing before implementation of Security measures

S.No	Types of Attacks possible on Fog Computing before implementing the security Measure	Percentage of Vulnerability
1	Advanced persistent Threats	15
2	Access Control Issue	30
3	Account Hijacking	16
4	Denial of services	21
5	Data Breaches	18
Vulnerability before the implementation of Proposed Security Measures		100

Table 1. Types of possible Attacks on Fog Computing before implementing the Security Measures.

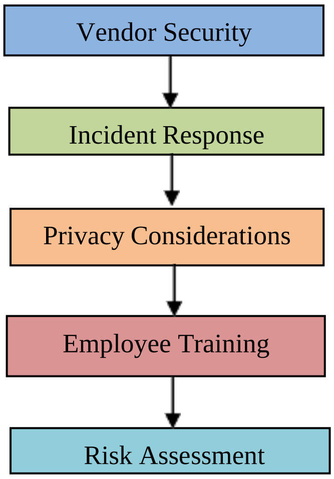


Fig.2. Various types of Fog Computing Measures

S.No	Types of Attacks possible on Fog Computing after implementing the security Measure	Percentage of Vulnerability
1	Vendor Security Assurance	6
2	Incident Response Plan	5
3	Privacy Considerations	8
4	Employee Training	4
5	Risk Assessment	2
6	Safe Region	75

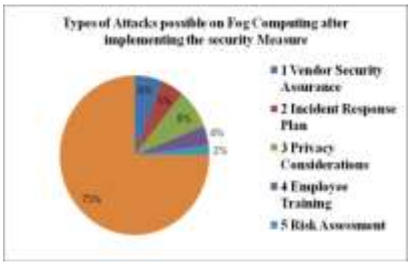


Fig 3. Measures in Fog Computing after implementation of security Measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols /firewalls which are unable to protect the vulnerabilities of Fog Computing. Hackers/introduces are continuously making attempts to gain the unauthorized access of Fog Computing using various attacks. Fog Computing devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Fog Computingseveral new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCE

[1] Frank Alexander Kraeme et.al, “Fog Computing in Healthcare–A Review and Discussion”,IEEE,15.May.2017,DOI: 10.1109/ACCESS.2017.2704100, Electronic ISSN: 2169-3536

[2] Taj-Aldeen Naser Abdali et.al, “Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues”,IEEE,19 May 2021, DOI: 10.1109/ACCESS.2021.3081770, Electronic ISSN: 2169-3536

[3] Fatemeh Jalali et.al,” Fog Computing May Help to Save Energy in Cloud Computing”,IEEE,23 March 2016, DOI: 10.1109/JSAC.2016.2545559, Electronic ISSN: 1558- 0008

[4] Manoj Muniswamaiah et.al,” Fog Computing and the Internet of Things (IoT): A Review”,IEEE, 26 June 2021, DOI: 10.1109/CSCloud-EdgeCom52276.2021.00012, Electronic ISBN:978-1-6654-4377-7

[5] Shanhe Yi et.al,” Fog Computing: Platform and Applications”,IEEE, 13 Novembe 2016, DOI: 10.1109/HotWeb.2015.22, Electronic ISBN:978-1-4673-9688-2

[6] Asma N. Elmoghrapi et.al,” Fog Computing or Cloud Computing: a Study”,IEEE, 06 July 2022, DOI: 10.1109/ICEMIS56295.2022.9914131,Electronic ISBN:978-1-6654-5436-0

[7] Ashkan Yousefpour et.al,” Fog Computing: Towards Minimizing Delay in the Internet ofThings”, IEEE, 30 June 2017, DOI: 10.1109/IEEE.EDGE.2017.12, Electronic ISBN:978-1-5386-2017-5

[8] Pooyan Habibi et.al,” Fog Computing: A Comprehensive Architectural Survey”, 25 March 2020, DOI: 10.1109/ACCESS.2020.2983253, Electronic ISSN: 2169-3536

[9] Munam Ali Shah et.al,” Delay-Aware Accident Detection and Response System Using Fog Computing”, 01 May 2019, DOI: 10.1109/ACCESS.2019.2910862, Electronic ISSN: 2169-3536

[10] Syed Usman Jamil et.al,” Accident Management System using Fog Computing”, 9 December 2019, DOI: 10.1109/ICOSST48232.2019.9043923, Electronic ISBN:978-1-7281-4613-3

[11] Bilal Khalid Dar et.al,” Fog Computing based Automated Accident Detection and Emergency Response System using Android Smartphone”, 22 November 2018, DOI: 10.1109/ICET.2018.8603557, Electronic ISBN:978-1-5386-8143-5

[12] Dominik Soukup et.al,”Security Framework for IoT and Fog Computing Networks”, 14 December 2019, DOI: 10.1109/I-SMAC47947.2019.9032592, Electronic ISBN:978-1-7281-4365-1

[13] Mohammad Aazam et.al,” E-HAMC: Leveraging Fog computing for emergency alert service”, 27 March 2015, DOI: 10.1109/PERCOMW.2015.7134091, Electronic ISBN:978-1-4799-8425-1.

Security Repercussions in Cloud Computing

P.HAFSA BEGUM
23CSC31, Student, M.Sc.(Computer Science)
Department of Computer Scince
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
pathanhafsabegum@gmail.com

CH.SOWMYA
Teaching Assistant
Department of Computer Science
P.B.Siddhartha College of Arts and Science
Vijayawada, A.P, India
sowmya@pbsiddhartha.ac.in

K.MONIKA
23CSC12, Student, M.Sc.(Computer Science)
Dept. of Computer Science
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
monikakorivi91@gmail.com

ABSTRACT: Cloud Computing Means Storing and Accessing the Data and Programs on Remote Servers That Are Hosted on The Internet Instead of The Computer's Hard Drive or Local Server. Cloud Computing Is Also Referred to As Internet-Based Computing, It Is A Technology Where the Resource Is Provided as A Service Through the Internet to The User. The Data Which Is Stored Can Be Files, Images, Documents, Or Any Other Storable Document. Cloud Computing Has Taken Its Place All Over the It Industries. It Is an On-Demand Internet-Based Computing Service That Provides the Maximum Result with Minimum Resources Cloud Computing Provides A Service That Does Not Require Any Physical Close to The Computer Hardware. Cloud Computing Is A Product of Grid, Distributed, Parallel, And Ubiquitous Computing. This Paper Introduces the Concepts, History Pros, And Cons of Cloud Computing. Now Coming to Iot, It Can Be Any Device Equipment, Or Object Which Connects Us with The Cloud Using the Internet or With Another Device That Is Connected. It Has Sensors, Processing Ability, Software, And Many Technologies Which Can Be Used to Share and Fetch Data or Information with Other Devices and Servers Over the Internet. Nowadays Big Companies Are Using Cloud Services for Storing Their Data Because It Is Easy to Manage Their Data Easily Without Any Additional Costs. Cloud Computing Provides Us the Flexibility to Play with Our Data and Gives Us More Freedom with Storage, Access, And Management. In This Paper, We Will See the Advantages and Disadvantages of Using the Cloud, How Iot Is Useful in Cloud Systems, And How We Can Overcome the Problems Related to The Cloud.

KEYWORDS: Malware, Accessing the Data, Network, Security, Authentication.

I. INTRODUCTION

In cloud computing, Cloud Computing concept has emergedfrom the distributed software architecture. Cloud computed technology is aimed to provide hosted services over the internet. In recent years, cloud computing in Information Technology has given rise to various new user communitiesand markets [1].

Cloud computing is an on-demand service, through internet different servers physical and virtual. It is more hosted at remote data and managed by CSP.CSP provides some services subscription-based or fees or bills according to usage or user. By using the cloud, we can get rid of purchasing, installing, and managing our infrastructure. Thismakes it easy for an organization to purchase and configure supporting hardware and make them use enterprise applications within minutes. we can scale capacity up and down according to response to spikes and dips in traffic. Over the years, with the development in Information Technology Industry, the demand for storing and computing resources growing bigger in the marketplace [2]. Cloud Computing is a network-built handling invention where information is provided to customers on demand. CloudComputing is a registering phase for dissemination of advantages and assets that involve structures, programming,applications, introduction and commerce. Distributed computing is a robotic supply of handling assets [3]. Cloud computing is everywhere. Pick up any tech magazine or visit almost any IT website or blog and you'll be sure to see talk about cloud computing. The only problem is that not everyone agrees on what it is. Ask ten different professionals what cloud computing is, and you'll get ten different answers. And is cloud computing even worth all the hype? Some people don't think so. In fact, in 2008Oracle CEO Larry Ellison chastised the whole issue of cloud computing, saying that the term was overused and being applied to everything in the computer world [4]. Cloud computing is a radical new IT delivery and business model. Users can use cloud services when and where they need them and, in the amount, they need them, and pay only forthe resources used. It offers huge computing power, on-demand scalability, and utility-like availability at low cost [5]. At present, there are many definitions of cloud computing in industry and academia, but there is no unified concept yet. Its core content is to provide computing, storage and network resources through the network, and provide users with various computing services convenientlyand on demand [6].

a. Cloud and edge computing are currently undergoing a substantive transformation on several fronts, from applications to hardware, and from architectures to devices. Paradigms such as computing in virtualization- based architectures, issues on geographic constraints fordeploying clouds, and the use of SDN/NFV in clouds [7].
b. Cloud computing has changed software infrastructures and business models of Internet services with technologies to provide and manage abundant resourcesof computation and data storage over the network at relatively low amortized operation costs [8].
c. The term "cloud computing" refers to the utilization of a set of infrastructure, data, applications, and services made up of networks of computer, informational, and storage resources. Businesses can benefit from a number of benefits from cloud computing, including resource elasticity, a decrease in the requirement for significant upfront infrastructure investments and adecrease in total cost of ownership [9].
d. One vision of 21st century computing is that users will access Internet services over lightweightportable devices rather than through somedescendant of the traditional desktop PC [10].

II. RELATED WORK

There are several security risks to consider when making theswitch to cloud computing. Some of the top security risks ofcloud computing include:

1. Limited visibility into network operations
2. Malware
3. Compliance
4. Data Leakage
5. Inadequate due diligence
6. Data breaches
7. Poor application programming interface (API)

Risks in Cloud Computing:

1. Limited visibility into network operations

When moving workloads and assets to the cloud, organizations forfeit a certain level of visibility into network operations. This is because the responsibility of managing some of the systems and policies shifts to the cloud service provider. Depending on the type of service model being used, the shift of responsibility may vary in scope. As a result, organizations must be able to monitor their network infrastructure without the use of network-based monitoring and logging [11].

2. Malware

By moving large amounts of sensitive data to an internet-connected cloud environment, organizations are opening themselves up to additional cyber threats. Malware attacks are a common threat to cloud security, with studies showing that nearly 90% of organizations are more likely to experience data breaches as cloud usage increases. As cybercriminals continue to become increasingly savvy with their attack delivery methods, organizations must be aware of the evolving threat landscape [12].

3. Compliance

Data privacy is becoming a growing concern, and as a result, compliance regulations and industry standards such as GDPR, HIPAA, and PCI DSS are becoming more stringent. One of the keys to ensuring ongoing compliance is by overseeing who can access data and what exactly they can do with that access. Cloud systems typically allow for large-scale user access, so if the proper security measures (ie. access controls) aren't in place, it can be difficult to monitor access across the network.

4. Data Leakage

Data leakage is a growing concern for organizations, with over 60% citing it as their biggest cloud security concern. As previously mentioned, cloud computing requires organizations to give up some of their control to the CSP.

5. Inadequate due diliengce

The move to the cloud should not be taken lightly. Similar to a third-party vendor, when working with a cloud service provider, it's important to conduct thorough due diligence to ensure that your organization has a complete understanding of the scope of work needed to successfully and efficiently move to the cloud. In many cases, organizations are unaware of how much work is involved in a transition and the cloud service provider's security measures are often overlooked.

6. Data breaches

One of the most impactful security risks the cloud faces is the potential for a data breach. These are a result of poor security measures that allow malicious actors to gain access to sensitive data across cloud servers.

7. Poor API

If the cloud has poor application program interfaces (API), then servers run the risk of having data unwillingly exposed. When it comes to API, malicious actors will employ several strategies such as brute force attacks and denial-of-service attacks in order to weaken the integrity of the system.

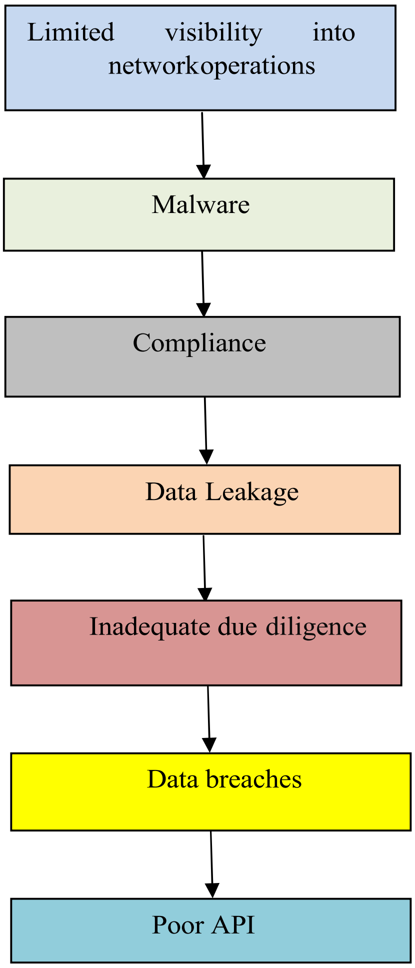


Fig.1. various risks in cloud computing

III. PROPOSED WORK

We propose the following security methods to prevent threats on Cloud Computing.

1) Security of Data

a. In terms of security concerns of cloud technology, we don't find answers to some questions. Mysterious threats like website hacking and virus attack are the biggest problems of cloud computing data security.

b. Before utilizing cloud computing technology for a business, entrepreneurs should think about these things. Once you transfer important data of your organization to a third party, you should make sure you have a cloud security and management system.

c. Cybersecurity experts are more aware of cloud security than any other IT professional. According to Crowd Research Partners survey, 9 out of 10 cybersecurity experts are concerned regarding cloud security. Also, they are worried about the violation of confidentiality, data privacy, and data leakage and loss.

d. Vendor Teradata also conducted a cloud analytics survey that reveals that 46% of those reviewed signified more security with no cloud computing challenge.

2) Insufficiency of Resources and Expertise

a. The inadequacy of resources and expertise is one of the cloud migrations challenges this year. As per the report by Right Scale, almost 75% of the respondent marked it as a challenge while 23% said that it was a serious challenge.

b. Although many IT employees are taking different initiatives to improve their expertise in cloud computing future predictions, employers still find it challenging to find employees with the expertise that they require.

c. According to the Robert Half Technology 2019 Salary Guide, businesses will only prioritize the tech employees with the knowledge and skills of the most recent growth in the cloud, mobile, open-source, big data, security, and other technologies in the upcoming years.

d. Some organizations are also expecting to win over the challenges of shifting to cloud computing by employing more workers with certifications or skills in cloud computing. Industry professionals also suggest providing training of present employees to make them more productive and speedier using the trendiest technology.

3) Complete Governance over IT Services

a. IT always doesn't have full control over provisioning, infrastructure delivery, and operation in this cloud-based world. This has raised the complicacy of IT to offer important compliance, governance, data quality, and risk management.

b. To eradicate different uncertainties and difficulties in shifting to the cloud, IT should embrace the conventional control and IT management procedures to incorporate the cloud. Ultimately, basic IT teams' role in the cloud has emerged over the last few years.

c. Alongside the business unites, core IT plays an increasing role in the mediation, preference, and control over cloud services. Moreover, third-party cloud computing or management providers are gradually offering best practices and government support.

4) Cloud Cost Management

a. The Right Scale report revealed that for a few companies, handling cloud spending has passed security as the biggest cloud computing challenge. As per their anticipations, organizations are ruining nearly 30% of the money they invest in the cloud.

b. Companies make several mistakes that can increase their expenses. Sometimes, IT professionals like developers turn on a cloud instance implied to be utilized for some time and forget to turn it off again. And some companies find themselves hindered by the hidden cloud costing packages that provide numerous discounts that they might not be using.

Using cloud spending management challenges, several tech solutions can help organizations. For instance, automation, cloud spending management solutions, serverless services, containers, autoscaling features, and numerous management tools provided by the cloud vendors may help lower the possibility of the issue. Furthermore, some companies have been succeeded by building a core cloud team for handling usage and costs.

5) Dealing with Multi-Cloud Environments

a. These days, maximum companies are not only working on a single cloud. As per the Flexera 2023 State of the Cloud Report, nearly 87% of the companies are following a multi-cloud strategy and 72% already have their hybrid cloud tactic that is combined with the public and private cloud. Furthermore, organizations are utilizing five distinct public and private clouds.

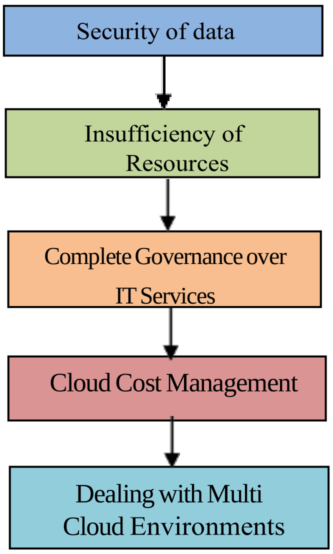

Security of data
Insufficiency of Resources
Complete Governance over IT Services
Cloud Cost Management
Dealing with Multi Cloud Environments

Fig.2.various measures in cloud computing

Algorithm:

1. Begin
2. Identify Potential Fog Computing Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End

IV. RESULT & ANALYSIS

S. No.	Type of Attacks possibleon cloud computing before implementing the security Measures	Percentage of Vulnerability
1	Limited visibility into network operations	20
2	Malware	30
3	Compliance	14
4	Data leakage	15
5	Inadequate due diligence	10
6	Data Breaches	6
7	Poor API	5
Vulnerability before the implementation of proposed Security Measures		100

Table 1. Types of possible Attacks on cloud computing before implementing the Security Measures

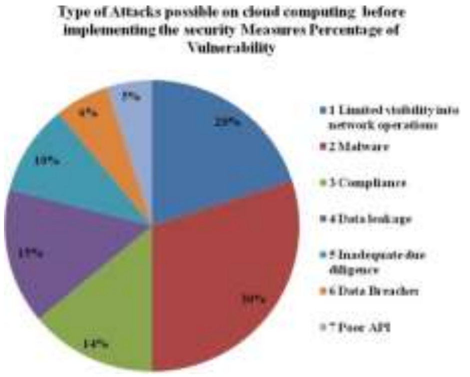


Fig.3. Risks before implementing of Security Measures

S.No.	Type of Attacks possible on cloud computing after implementing the security Measures	Percentage of Vulnerability
1	Security of Data	10
2	Insufficiency of Resources and Expertise	5
3	Complete Governance over IT Services	6
4	Cloud Most Management	2
5	Dealing with Multi-Cloud Environments	7
Vulnerability before the implementation of proposed Security Measures		30

Table 2. Types of possible Attacks on cloud computing after implementing the Security Measures

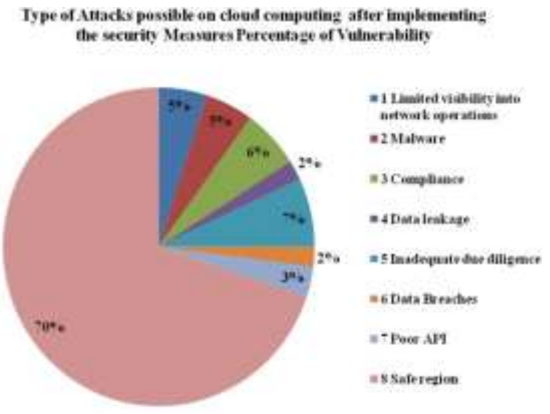


Fig. 4. Risks after implementation of Security Measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols /firewalls which are unable to protect the vulnerabilities of Fog Computing. Hackers/introduces are continuously making attempts to gain the unauthorized access of Fog Computing using various attacks. Fog Computing devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Fog Computingseveral new security measures, protocols and firewalls needsto developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] bader alouffi ,"a systematic literature review on cloud computing security: threats and mitigationstrategies",14april2021 ,doi: 10.1109/access.2021.3073203,electronic issn: 2169-3536

[2] neeraj single, "a review paper on cloud computing",23-24december2022, DOI: 10.1109/cisct55310.2022.1004657, electronic isbn:978-1-6654-7416-0

[3] gurmeher singh puri, "a review on cloud computing",10-11january2019, DOI: 10.1109/confluence.2019.8776 907, electronic isbn:978-1-5386-5933-5

[4] shyam patida, "a survey paper on cloud computing", 07-08 january 2012, DOI: 10.1109/acct.2012.15, isbn:978-1-4673-0471-9

[5] san murugesan, "cloud computing", 2016, DOI: 10.1002/9781118821930.ch1, electronic isbn:9781118821961.

[6] sanchuan luo, "application of cloud computing in data information system management ",14-16 October 2022, DOI: 10.1109/icinc58035.2022.00019, electronic isbn:979-8-3503-0969-0.

[7] nader f. mir, "cloud and edge computing", june 2020, DOI: 10.1109/mcomstd.2020.9139038, electronic issn: 2471-2833.

[8] sanae esseradi, "mobile cloud computing: current development and research challenges", 27- 30 may 2013, DOI: 10.1109/aiccsa.2013.6616482, electronic isbn:978-1-4799-0792-2

[9] divyansha garg, "cyber attacks in cloud computing environment", 01-03 june 2023, DOI: 10.1109/icces57224.2023.10192833, electronic isbn:979-8-3503-9663-8

[10] jing liu, "ccra: cloud computing reference architecture",24-29june2012, DOI: 10.1109/scc.2012.110

[11] savita devi, "study of architecture and issues in services of cloud computing", 17-18 december 2021, DOI: 10.1109/icac3n53548.2021.9725679, electronic isbn:978-1-6654-3811-7

[12] suyel namasudra , "cloud computing: fundamentals and research issues" ,05 october 2017, DOI: 10.1109/icrtccm.2017.49, electronic isbn:978-1-5090-4799-4

Challenges on Devops

M.Sumalatha,
23CSC24, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B. Siddhartha College of Arts & Science
Vijayawada, A.P, India
madalasumalatha1@gmail.com

Dr.A.Srisaila,
Asst. Professor,
Dept. of Information Technology,
V.R.Siddhartha College of Arts & Science, A.P, India.
a.srisaila@vrsiddhartha.ac.in

P.Anusha,
23CSC13, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
pajarlaanusha12@gmail.com

ABSTRACT: Devops Is the Combination of Cultural Philosophies, Practices, And Tools That Increases an Organization's Ability to Deliver Applications and Services at High Velocity: Evolving and Improving Products at A Faster Pace Than Organizations Using Traditional Software Development and Infrastructure Management Processes. This Speed Enables Organizations to Better Serve Their Customers and Compete More Effectively in The Market. Devops Is an Emerging Practice to Be Followed in The Software Development Life Cycle. The Name Devops Indicates That It's an Integration of The Development and Operations Team. It Is Followed to Integrate the Various Stages of The Development Lifecycle. Devops Is an Extended Version of The Existing Agile Method. Devops Aims at Continuous Integration, Continuous Delivery, Continuous Improvement, Faster Feedback and Security. This Paper Reviews the Building Blocks of Devops, Challenges in Adopting Devops, Models to Improve Devops Practices and Future Works on Devops.

KEYWORDS: Continuous Integration, Testing, Culture.

I. INTRODUCTION

The practices followed during the software development lifecycle play an important role. In the conventional development lifecycle, different teams will play their role at their level. Separate teams make the product life cycle lengthier and also the communication between the team's poor. This kind of development model is called the waterfall model. To break the walls between the teams and to enhance the dissemination of the information the new methodology Agile was discovered. Agile means "to move fast and easy". Agile process methodology improved the interaction between individual teams and improved collaboration. Some of the agile principles are Scrum, Extreme Programming, Lean, Kanban and out of these the Scrum was the first developed principle [1]. DevOps manifesto has been debated broadly among researchers and software engineering practitioners. DevOps is a defining software delivery standard which allows development and operations team work closely and minimize gaps between them.

Fig.1. Illustration of devops

DevOps is the theoretical perception of the agile development and agile operation discipline which combination of the software engineering practices. In addition, DevOps is a discipline that emphasizes on the collaboration of developers and operations department to unleased software product in frequently and rapid process to customers. Meanwhile, the delivery pipeline establishes the last portion of the supply chain for the software development life cycle [2]. Agile software development methods are gaining popularity in the industry. Their main advantage, as opposed to traditional development approaches, is their ability to respond to rapidly changing environments which makes them an attractive operating model for many companies. Additionally, product-oriented, agile teams are deemed to handle customer demands better, although an increasing disconnect between IT development and operation functions presents a bottleneck in this process and impedes the fast delivery of new software functionality. Organizations therefore turn to software delivery approaches like DevOps which aims to bridge this gap by combining both IT development and operations into cross-functional teams. Agile and DevOps are considered important methods for companies undergoing a digital transformation since they enable the delivery of innovative products or services via digital services platforms [3]. DevOps is an emerging practice that has been adopted in the software development cycle. It focuses on the convergence of standards between the Development teams and the Operations teams and it seeks to improve cooperation between both teams, hence the origin of the term [4]. DevOps tools and methods have also reduced the cultural and methodological divide between developers and operators, leading to the formation of many new organizational structures within software vendors, such as virtual teams composed of both developers and operators, and the establishment of new professional figures often referred to as DevOps engineers, who center their activity on tooling and automation across the whole application lifecycle [5]. DevOps is an organizational transformation that had its origin at the 2008 Agile Conference in Toronto, where P. Debois highlighted the need to resolve the conflict between development and operations teams when they had to collaborate to provide quick response time to customer demands. Later, at the O'Reilly Velocity Conference, two Flickr employees delivered a seminal talk known as "10+ Deploys per Day: Dev and Ops Cooperation at Flickr", which can be considered the starting point to extend agility beyond development [6]. Therefore, an architectural strategy based on modular development and distributed deployment is needed to support the construction of the company's platform. The current popular microservice architecture is an ideal solution to this problem [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in devops

Risks in devops:

1. **Test Automation:** Since writing new tests from scratch could delay launching your automated build process, you tend to use existing automated tests. The problem is that these tests are functional unit tests that developers use to make sure that what they build works [8].
2. **Tooling**: If user's feel the new tools make the process burdensome, start looking for their own alternatives. choosing the wrong CI/CD tool set is a risk you should avoid at all costs. if some tools are not properly configured, or integrated into the system, they will cause blockages [9].
3. **Security Risks**: Building a delivery pipeline is a crucial DevOps practie. One of the most important issues when building an automatic delivery pipeline is the risk of prioritizing convenience and efficiency over security. Proper enforcement of software security involves listening to the news [10].
4. **Organizational Uncertainty:** If no one knows what methodology they are following, what it necessitates, why it matters, and the expected goals and outcomes, the project is lost. Often this leads to everybody arguing over definitions and the way to use them [11].
5. **Poor Quality Code: Static** code analysis is a collection of algorithms and techniques used to analyze source code to automatically find errors or poor coding practices. Static code analysis, looks at applications in non-runtime environments.

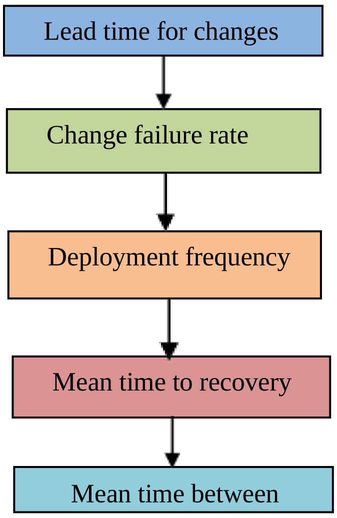


Fig.2.Various risks to devops

III. PROPOSED WORK

We propose the following security methods to prevent threats on devops.

1. **Lead time for changes:** High-performing teams typically measure lead times in hours, versus medium and low-performing teams who measure lead times in days, weeks, or even months.
2. **Change failure rate:** High-performing teams have change failure rates in the 0-15 percent range. The same practices that enable shorter lead times. Times test automation, trunk-based development, and working in small batches correlate with a reduction in change failure rates.
3. **Deployment frequency:** High-performing teams can deploy changes on demand, and often do so many times a day. Lower-performing teams are often limited to deploying weekly or monthly. The ability to deploy on demand.
4. **Mean time to recovery:** MTTR is the mean time to recovery, sometimes called mean time to restore. It is the time it takes to get a system operational following a fault. It became a standard measure of software delivery performance as part of the DORA metrics. When you perform well against all DORA metrics, you have working software sooner, happier employees, and a competitive advantage in your industry.
5. **Mean time between failures:** MTBF (mean time between failures) is the average time between repairable failures of a technology product. The metric is used to track both the availability and reliability of a product. The higher the time between failure, the more reliable the system.

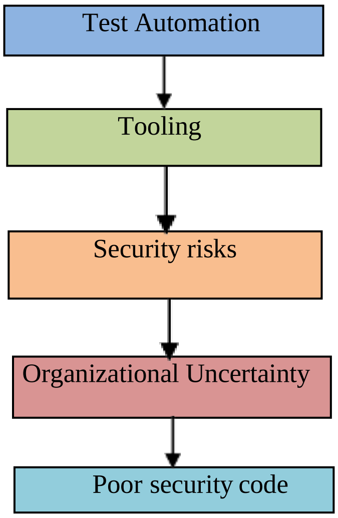


Fig. 3. Various measures to devops

Algorithm:

1. Begin
2. Identify Potential Fog Computing Security Threats.
3. Focus on the most probable Threats that could Harm
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized
7. End

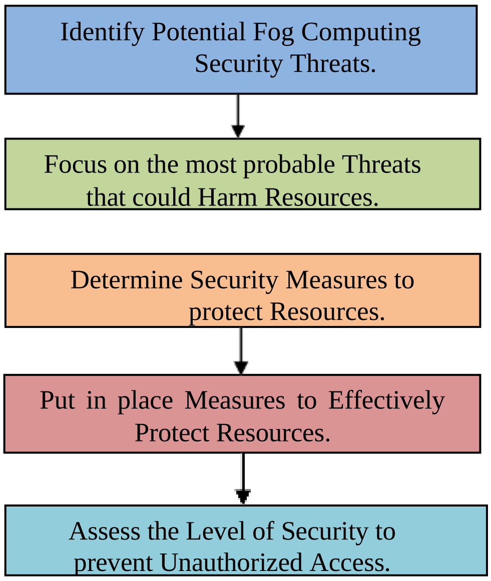

Identify Potential Fog Computing Security Threats.
Focus on the most probable Threats that could Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 4. Procedure to safeguard the resources of devops

IV. RESULT & ANALYSIS

S. No	Types of attacks possible on Fog Computing before implementing theSecurity Risks	Percentage of Vulnerability
1	Test automation	19
2	Tooling	23
3	Security risks	19
4	Organizational uncertainty	18
5	Poor security code	21
Vulnerability before the implementation ofproposed Security Risks		100

Table 1. Types of Possible Attacks on Fog Computing before implementing the Security Risks

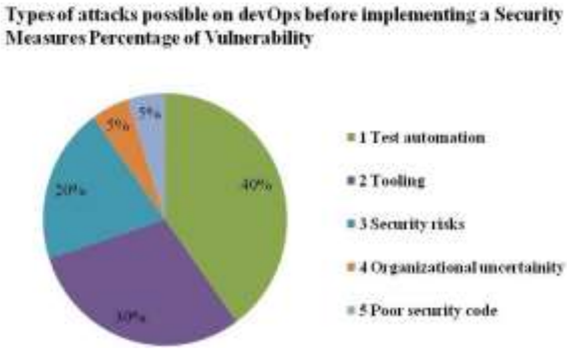


Fig. 5. Vulnerability before implementation of Security Measures.

S. No	Types of attacks possible onFog Computing after implementing the Security measures	Percentageof Vulnerability
1	Test automation	7
2	Tooling	5
3	Security risks	7
4	Organizational uncertainity	5
5	Poor security code	6
Vulnerability after the implementation of proposed SecurityMeasures		30

Table 2. Types of Possible Attacks on Fog Computing after implementing the Security Measures

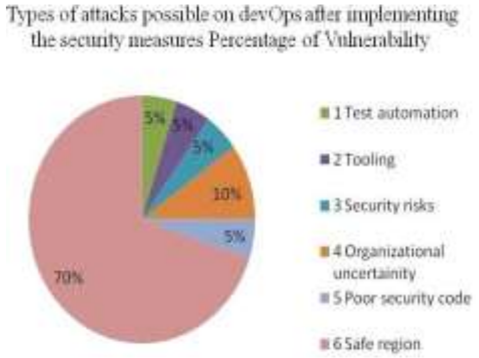


Fig .2. Vulnerability after implementation of Security Measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of devops. Hackers/ introduces are continuously making attempts to gain the unauthorized access of devops using various attacks. Devops devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of devops several new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Mayank Gokarnaet.al, “DevOps: A Historical Review and FutureWorks”,19February2021, DOI: 10.1109/ICCCIS51004.2021.9397235, Electronic ISBN:978-1-7281-8529-3.

[2] M.ZulfahmiTohet.al A Review on DevOps Adoption in Continuous Delivery Process”, 26August2021, DOI: 10.1109/ICSEC S52883.2021.00025, Electronic ISBN:978-1-6654-1407-4.

[3] JosvanHillegersberget.al, How DevOps capabilities leverage firm competitive, 03 September 2021,
DOI: 10.1109/CBI52690.2021.00025, Electronic ISBN:978-1-6654-2069-3.

[4] LucianodeAguiarMonteiroe.al,”A Proposal to System at ize Introducing DevOps”, 28 May 2021, DOI: 10.1109/ICSE Companion52605.2021.00124, ISBN:978-1-6654-1219-3.

[5] AhmadAlnafessahet.al, “Quality Aware DevOps Research: Where Do We Stand”, 09 March 2021, DOI: 10.1109/ACCESS. 2021.3064867 Electronic ISSN: 2169-3536.

[6] Daniel López Fernándezet.al, DevOps Team Structures: Characterization and Implications”, 06 August 202, DOI: 10.1109/TSE.2021.3102982 Electronic ISSN: 1939-3520.

[7] JiaxingXuan Micro serviceet.al, Publishing Technology Based on DevOps Architecture”, 15 October 2021, DOI: 10.1109/IT NEC52019.2021.9586904. Electronic ISBN:978-1-6654- 1599-6 Electronic ISSN: 2693-3128.

[8] Yuqing Wanget.al, “Test Automation Process Improvement in a DevOps Team”, 24 October 2020, DOI: 10.1109/ICSTW5029 4.2020.00057 Electronic ISBN:978-1-7281-1075-2.

[9] ChorMyeonggilet.al “The Security Risks of Cloud Computing”, 01-03August 2019, DOI: 10.1109/CSE/EUC.2019.00069, Electronic ISBN:978-1-7281-1664-8.

[10] John E.Ettlie “Environmental uncertainty and organization ai technology policy”, 1 February 1982, DOI: 10.1109/TEM.198 2.6447460 Electronic ISSN: 1558-0040.

[11] Hongkai Chen “Research on Network Information Security and Protection System”, 11December2022
DOI: 10.1109/TOCS56154.2022.10015993 Electronic ISBN:978-1-6654-7053-7.

[12] SafakBirol Estimating Lead Time Using Machine Learning Algorithms”, 08 October 2021, DOI: 10.1109/ASYU52992.202 1.9599012 Electronic ISBN:978-1-6654-3405-8.

Beyond Innovation : The Dark Side of Generative AI Security

P.Saniya Tahaseen,
23CSC14, Student,
M.Sc.(ComputerScience),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
saniyatahaseen9800@gmail.com

K.Kishore,
23CSC09, Student,
M.Sc.(ComputerScience),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
kishork1026@gmail.com

J.Swarna Latha,
23CSC08, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
swarnalatha08@gmail.com

ABSTRACT: Generative Artificial Intelligence (AI) Has Emerged as A Transformative Field That Enables Machines to Exhibit Creativity and Produce Novel Content Across Various Domains. This Abstract Explores the Evolution, Methodologies, And Applications of Generative AI. Initially Rooted in Probabilistic Modeling, Generative AI Has Evolved with The Advent of Deep Learning and Neural Networks, Allowing Machines to Generate Content Indistinguishable from Human-Created Artifacts. This Paper Delves Into The Fundamental Concepts Behind Generative Adversarial Networks (Gans), Variational Autoencoders (Vaes), And Other Prominent Models, Elucidating Their Architectures And Training Processes. It Examines How These Models Learn from Vast Datasets, Capture Intricate Patterns, And Subsequently Generate Diverse Outputs, Including Images, Music, Text, And More.

KEYWORDS: Malicious, Access Control, Network, Security, Authentication.

I. INTRODUCTION

Artificial intelligence (AI) has the potential to vastly improve the metaverse by automating intelligent decision-making and creating highly customized user experiences. Web3, with its distributed network architecture, provides consumers with enhanced privacy and security when conducting financial transactions online [1], [2], [3]. In addition, the immutable data storage and transfer mechanisms made possible by blockchain technology guarantee data security and integrity. In the age of Web3, generative AI technologies like Chat Generative Pre-Trained Transformer (ChatGPT) have the capacity to become productivity tools by addressing problems with digital assets and content production and filling in essential gaps in Web3's evolution [4]. Generative AI technologies are expected to accelerate the advent of the Web3 era by offering more reliable and convenient productivity tools for Web3 creators and contributors. With the advent of generative AI technologies, such as ChatGPT, there has been widespread attention in the industry towards its creativity and flexibility. The efficiency and quality of content production and dissemination may be greatly improved with the help of ChatGPT based on deep learning models, which can generate content in a wide variety of contexts and fulfill a wide range of needs. In addition to these benefits, ChatGPT can facilitate eliminating obstacles, enhancing human understanding and creativity, and generating priceless insights and innovations. ChatGPT can also use multi-modal AI technologies to analyze, interpret, and generate information in greater detail by leveraging different perceptual modes [5], [6], [7]. This will allow for real- time perception and response to content and provide flexible feedback, ultimately leading to the creation of more rich and diverse forms of content. Technologies such as virtual characters, speech synthesis, and image generation more rich and diverse forms of content. Technologies such as virtual characters, speech synthesis, and image generation process. Technology advancements in AI for Generative Content (AIGC) have led to the emergence of critical technologies like ChatGPT as components of the metaverse engine layer, considerably easing the process of creating high-quality material in the metaverse [8]. Currently, the metaverse's content scale has not yet met user demands, and the cost of building metaverse spaces remains high, affordable only for a few companies. Moreover, virtual spaces created with substantial investments often lack excitement, openness, and refinement. Yet, the price of constructing metaverse environments can be drastically decreased if AI can assist creators in lowering the barriers, such as providing consistent scenes with basic descriptions [9], [10], [11].

Fig.1. Illustration of Generative AI

II. RELATED WORK

Risks of Generative AI:

1. Data Overflow:

People can enter any type of data into Generative AI services via open text boxes, including sensitive, private or proprietary information. Take code-generating services like GitHub Copilot as an example. The code sent to this service could contain not just a company's confidential intellectual property, but also have sensitive data like API keys that have special access to customer information.

2. IP Leak:

Another serious concern is IP leakage and confidentiality when using generative AI, adding that the ease of use of web- or app-based AI tools risks creating another form of shadow IT. Given that these online generative AI apps send and process data over the internet, using a VPN can provide an extra layer of security, masking your IP address and encrypting the data in transit.

3. Synthetic Data:

Generative AI can create synthetic data that looks a lot like real data, which can lead to concerns about people being able to figure out who the data came from. Synthetic data could have small patterns or details that might lead to people or sensitive features being identified.

4. Accidental Leaks:

Generative models, especially ones based on text or images, can unintentionally include information from the training data that shouldn't have been revealed. This could be personal information or confidential business data.

5. AI Misuse and Malicious Attacks:

Generative AI could potentially be misused by malicious actors to create deep fakes or generate misleading information, contributing to the spread of fake news and disinformation. Moreover, if AI systems are not adequately secured, they could become a target for cyberattacks, creating additional data security concerns.

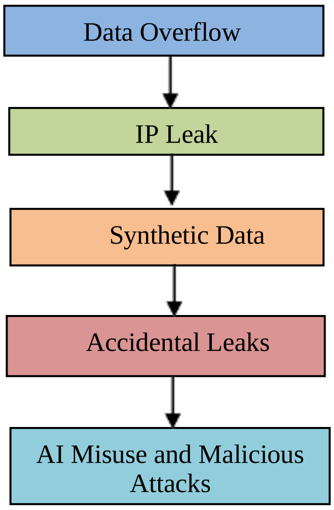


Fig 2: Various risks of Generative AI

III. PROPOSED WORK

Measures of Generative AI:

1. **Personalize to lower risks:** Companies should be proactive in deciding on tech providersand if possible, develop internal AI solutions to lower the riskof data breaches. If you can't internalize these solutions, Evaluate the level of sensitivity of the data used in these toolsbefore deciding the type of service to use - publicly availablemodels, local deployment, cloud, etc.
2. **Diminishing the attack surface:** You can do this by ensuring that all AI-based tools accessing your core systems have least privileged access, are monitored on a daily basis and also by removing unused connections.
3. **Constantly examine the data:** Companies should consider how their data is being used and retained by the solution they are implementing. Track solutions' behavior so you can detect anomalies as your data is being shared over time.
4. **Performance makes ideal:** Test these tools first within your organization before utilizing them for outside consumption. Using an AI tool that you're not familiar with for a customer-facing initiative could backfire and negatively impact the business.
5. **To Get a full record of AI-tools within the association and execute both on boarding and off boarding processes:** When on boarding, look at inventory and see what tools and data they have access to. If a tool isn't valuable or is dangerous, make sure during the off-boarding process that it'snot only disconnected from all parts of the environment but also deletes your data.

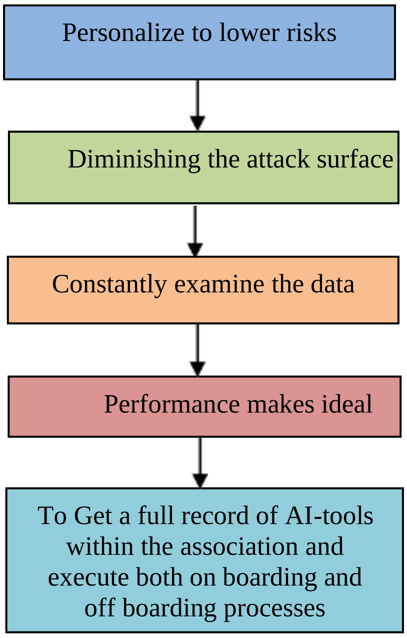
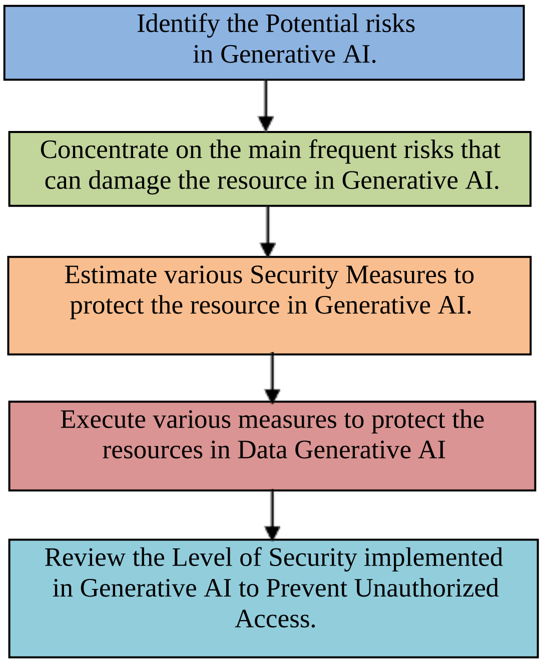

Personalize to lower risks
Diminishing the attack surface
Constantly examine the data
Performance makes ideal
To Get a full record of AI-tools within the association and execute both on boarding and off boarding processes

Fig 3: Various Measures of Generative AI

Algorithm:

1. Begin
2. Identify the Potential risks in Generative AI.
3. Concentrate on the main frequent risks that can damage the resource in Generative AI.
4. Estimate various Security Measures to protect the resource in Generative AI.
5. Execute various measures to protect the resources in Data Generative AI.
6. Review the Level of Security implemented in Generative AI to Prevent Unauthorized Access.
7. End.



Identify the Potential risks in Generative AI.

Concentrate on the main frequent risks that can damage the resource in Generative AI.

Estimate various Security Measures to protect the resource in Generative AI.

Execute various measures to protect the resources in Data Generative AI

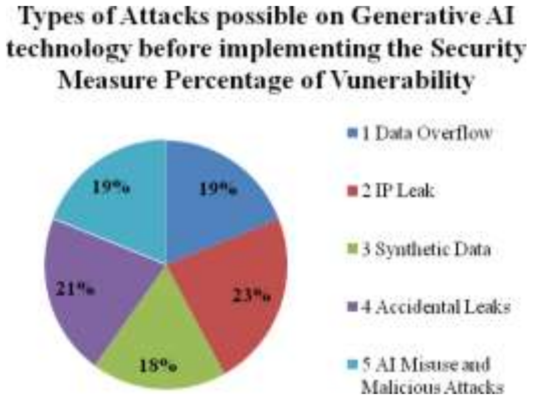
Review the Level of Security implemented in Generative AI to Prevent Unauthorized Access.

Fig. 4. Procedure to safeguard the resources of Generative AI

IV. RESULT & ANALYSIS

S.No	Types of Attacks possible on Generative AI technology beforeimplementing the SecurityMeasures	Percentage of Vulnerability
1	Data Overflow	19
2	IP Leak	23
3	Synthetic Data	18
4	Accidental Leaks	21
5	AI Misuse and Malicious Attacks	19
Vulnerability before the implementation ofproposed security measures		100

Table 1. Types of Possible Attacks on Generative AI before implementing the Security Risk



S.No	Types of Attacks possible on Generative AI technology After implementing the Security Measures	Percentage of Vulnerability
1	Data Overflow	7
2	IP Leak	8
3	Synthetic Data	6
4	Accidental Leaks	3
5	AI Misuse and Malicious Attack	2
Vulnerability after the implementation of proposed security measures		26

Table 2. Types of possible Attack on Generative AI after implementing the Security Measures

Fig.1 Vulnerability before implementing the security measures to generative AI

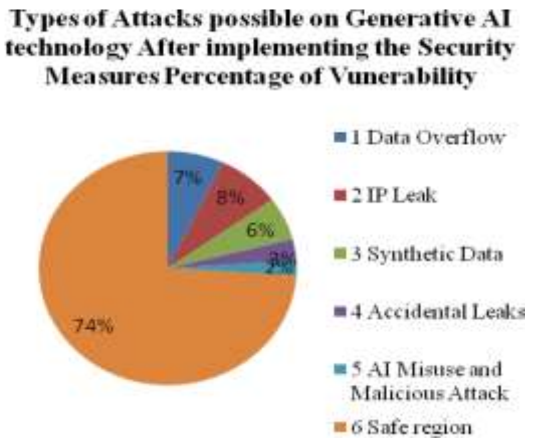


Fig.2. Risk after implementation of Security Measures to Generative AI

V. CONCLUSION AND FUTURE WORK

Even though several securities are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of Generative AI. Hackers / introduces are continuously making attempt to gain the unauthorized access of Generative AI using various attacks. As Generative AI usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Generative AI several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] S. Mondal et. al, “Generative AI: How to bell the cat? A theoretical review of generative artificial intelligence towards digital disruption in all walks of life”, IEEE, 17 March2023, DOI: https://doi.org/10.3390/technologies110200 44.

[2] M. Hitchens et. al, “Generative AI: On the design of a flexible delegation model for the Internet of Things using blockchain IEEE Trans. Ind. Inf., 16 (5) (2019), pp. 3521-3530.

[3] M. Jovanovic et. al, “Generative AI: Generative artificial intelligence: trends and prospects Computer (Long Beach Calif), 55 (10) (2022), pp. 107-112, DOI: 10.1109/MC.2022.3192720.

[4] J. Perkins Immersive metaverse experiences in decentralized 3d virtual clinical spaces: artificial intelligence-driven diagnostic algorithms, wearable internet of medical things sensor devices, and healthcare modeling and simulation tools Am. J. Med. Res., 9 (2) (2022), pp. 89-104.

[5] Gill S. et. at, “ChatGPT: vision and challenges Internet of Things and Cyber-Physical Systems, 2023.

[6] Q. Cai, H. et. al, “A survey on multi-modal data-driven smart healthcare systems: approaches and applications” IEEE Access, 7 (2019), pp. 133583-133599.

[7] P.P Ray ChatGPT: a comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope [J] Internet Things Cyber-Phys. Syst. (2023).

[8] A. Baía Reis, M Ashmore from video streaming to virtual reality worlds: an academic, reflective, and creative study on live theatre and performance in the metaverse Int. J. Performance Arts Digital Media, 18 (1) (2022), pp. 7-28 [9] A.A Gaafar Metaverse in architectural heritage documentation & education Adv. Ecol. and Environ. Res., 6 (10) (2021), pp. 66-86.

[10] R Godwin-Jones Emerging spaces for language learning: AI bots, ambient intelligence, and the metaverse Lang. Learn. Technol., 27 (2) (2023), pp. 6-27.

[11] W.M. Lim, A. Gunasekara, J.L. Pallant, J.I. Pallant, E. Pechenkina Generative AI and the future of education: ragnarök or reformation? A paradoxical perspective from management educators Int. J. Manage. Edu., 21 (2) (2023), Article 10079.

Quantum Computing : A New Revolution in Computing Technology

P.Satya Naga Vara Prasad,
23CSC15, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
satyaprasadpujari3699@gmail. com

G.Radha Krishna,
23CSC23, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
radhakrishna1115@gmail. com

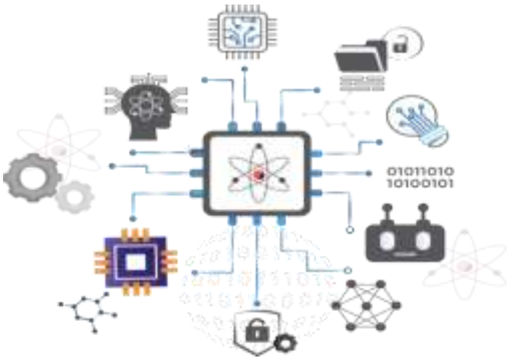
P.Rama Krishna,
23CSC25, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
ramakrishnavanamadi1020 @gmail.com

ABSTRACT: The Development of Quantum Computers Over the Past Few Years Is One of The Most Significant Advancements in The History of Quantum Computing. D-Wave Quantum Computer Has Been Available for More Than Eight Years. IBM Has Made Its Quantum Computer Accessible Via Its Cloud Service. Also, Microsoft, Google, Intel, And NASA Have Been Heavily Investing in The Development of Quantum Computers and Their Applications. The Quantum Computer Seems to Be No Longer Just for Physicists and Computer Scientists, But Also for Information System Researchers. This Paper Introduces the Basic Concepts of Quantum Computing and Describes Well-Known Quantum Applications for Non-Physicists. The Current Status of The Developments in Quantum Computing Is Also Presented.

KEYWORDS: Quantum Computer, Quantum Gate, QKD, Shor, Grover

I. INTRODUCTION

Today's computers both in theory (Turing machines) and practice (PCs, HPCs, laptops, tablets, smartphones, . . .) are based on classical physics. They are limited by locality (operations have only local effects) and by the classical fact that systems can be in only one state at the time. However, modern quantum physics tells us that the world behaves quite differently. A quantum system can be in a superposition of many different states at the same time, and can exhibit interference effects during the course of its evolution. Moreover, spatially separated quantum systems may be entangled with each other and operations may have "non-local" effects because of this. Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles. It combines two of the most important strands of 20th-century science: quantum mechanics (developed by Planck, Einstein, Bohr, Heisenberg, Schrodinger and others in the period 1900–1925) and computer science (whose birth may be dated to Turing's 1936 paper [1]). An important objective is to find quantum algorithms that are significantly faster than any classical algorithm solving the same problem. Quantum computation started in the early 1980s with suggestions for analog quantum computers by Yuri Main [2] (and appendix of [3]), Richard Feynman [4,5], and Paul Benioff [6], and reached more digital ground when in 1985 David Deutsch defined the universal quantum Turing machine [7]. See Preskill [8] for more on this early history. The following years saw only sparse activity, notably the development of the first algorithms by Deutsch and Jozsa [9] and by Simon [10], and the development of quantum complexity theory by Bernstein and Vazirani [11]. However, interest in the field increased tremendously after PeteShor's very surprising discovery of efficient quantum algorithms for the problems of integer factorization and discrete logarithms in 1994 [12,13], which was inspired by Simon's work. Since most of current classical cryptography is based on the assumption that these two problems are computationally hard, the ability to actually build and use a quantum computer would allow us to break most current classical cryptographic systems, notably the RSA system [14]. In contrast, a quantum form of cryptography due to Bennett and Brassard [15] is unbreakable even for quantum computers Here are three reasons to study quantum computers, from practical to more philosophical: 1. The process of miniaturization that has made current classical computers so powerful and cheap, has already reached micro-levels where quantum effects occur. Chipmakers tend to go to great lengths to suppress those quantum effects, forcing their bits and logical operations 1 to behave classically, but instead one might also try to work with them enabling further miniaturization. 2. Making use of quantum effects allows one to speed up certain computations enormously (sometimes exponentially), and even enables some things that are impossible for classical computers. The main purpose of these lecture notes is to explain these advantages of quantum computing (algorithms, crypto, etc.) in detail. 3. Finally, one might say that the main goal of theoretical computer science is to "study the power and limitations of the strongest-possible computational devices that Nature allows us." Since our current understanding of Nature is quantum mechanical, theoretical computer science should arguably be studying the power of quantum computers, not classical ones.



II. RELATED WORK

Security risks and challenges of quantum computing:

1. Shor's Algorithm and Cryptography:

a. Shor's algorithm, a quantum algorithm developed by mathematician Peter Shor, has the potential to efficiently factor large numbers.

b. This poses a significant threat to widely used public-key cryptography systems, such as RSA and ECC, which rely on the difficulty of factoring large numbers for security.

c. Once large-scale, fault-tolerant quantum computers become available, they could break these cryptographic systems, compromising the security of sensitive data.

2. Quantum-Safe Cryptography:

a. The threat to classical cryptography from Shor's algorithm has led to the development of quantum- safe or post-quantum cryptographic algorithms.

b. Transitioning to these quantum-resistant algorithms is crucial to maintaining the security of data and communications in a future where quantum computers are prevalent.

3. Data Security:

a. Quantum computers could potentially be used to break encryption and security protocols in place today.

b. This includes not only the decryption of previously encrypted data but also the potential to intercept and decrypt data transmitted over secure communication channels.

4. Block chain Security:

a. Quantum computing could pose a threat to the security of block chain technologies, especially those relying on existing cryptographic algorithms.

b. Many crypto currencies and block chain systems use public-key cryptography for securing transactions, and if these cryptographic schemes become vulnerable to quantum attacks, the security of block chain networks could be compromised.

5. Quantum Security:

a. Quantum computers could potentially break widely used cryptographic hash functions.

b. This raises concerns about the integrity of digital signatures, certificates, and other forms of data verification, impacting the security and authenticity of digital information.

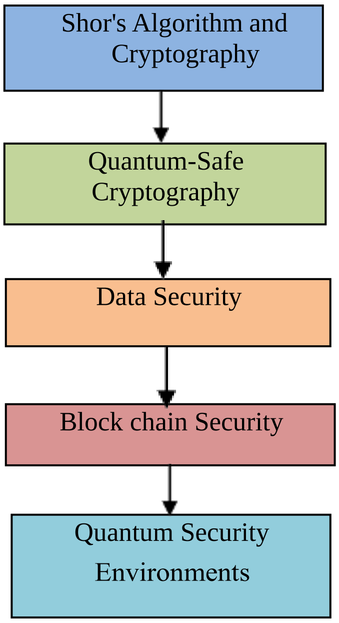

Shor's Algorithm and Cryptography
Quantum-Safe Cryptography
Data Security
Block chain Security
Quantum Security Environments

Fig.1. various security risks in quantum computing

III. PROPOSED WORK

Measures to overcome from quantum computing:

1. **Transition to quantum-resistant or post- quantum cryptographic algorithms:**
   a. Researchers are actively working on developing cryptographic algorithms that remain secure in the presence of quantum computers.
   b. It's important to start adopting these quantum-resistant algorithms to ensure the long-term security of sensitive data.
2. **Implement Quantum Key Distribution:**
   a. QKD is a method that uses quantum properties to secure a communication channel.
   b. It allows two parties to produce a shared random secret key, which can then be used to encrypt and decrypt messages.
   c. QKD provides a level of security that is theoretically immune to quantum attacks.
3. **Explore Quantum-Safe Network Protocols:**
   a. Develop and implement network protocols that are resistant to attacks from quantum computers.
   b. This includes ensuring the security of authentication, integrity, and confidentiality mechanisms.
4. **Choose Quantum-Resistant Hash Functions:**
   a. Hash functions are widely used in various security protocols.
   b. Select cryptographic hash functions that are resistant to attacks by quantum algorithms, ensuring the integrity and authenticity of data.

S.No	Types of Attacks possible on Quantum Computing Technology before implementing the Security Measures	Percentage of vulnerability
1.	Shor's Algorithm and Cryptography	21
2.	Quantum-Safe Cryptography	19
3.	Data Security	18
4.	Block chain Security	22
5.	Quantum Security	2
Vulnerability before the Implementation of Proposed Security Measures		100

Table 1. Types of possible attacks on Quantum Computing before implementing the Security Measures

5. **Regular Security Assessments:**
   a. Continuously assess and update security protocols and infrastructure to incorporate advancements in quantum-safe cryptography.
   b. Regularly reviewing and updating security measures is essential in the face of evolving threats.

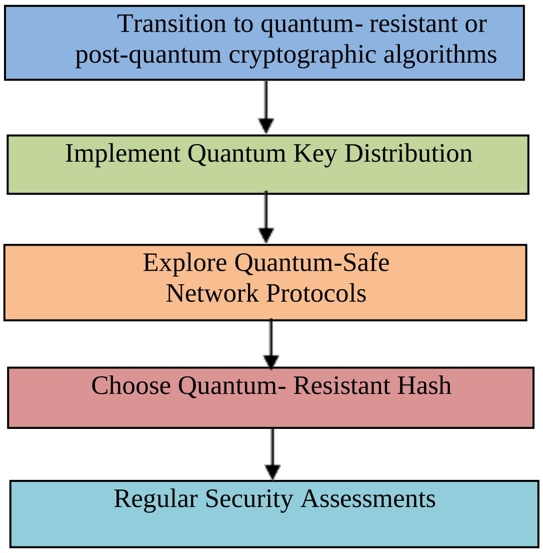
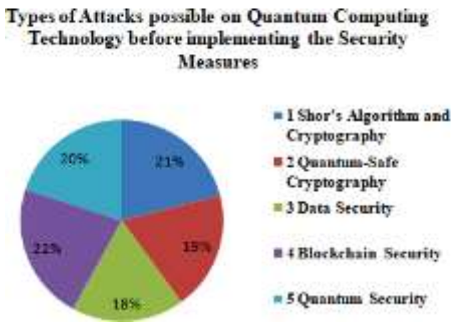

Transition to quantum- resistant or post-quantum cryptographic algorithms
Implement Quantum Key Distribution
Explore Quantum-Safe Network Protocols
Choose Quantum- Resistant Hash
Regular Security Assessments

Fig.2. various measures of quantum computing

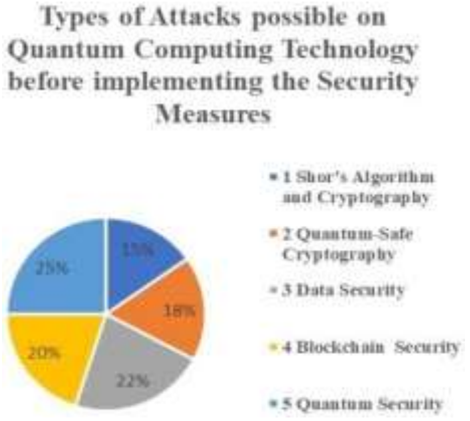
Algorithm:

1. Begin
2. Identify the Potential risks in Quantum Computing.
3. Concentrate on the main frequent risks that can damage the resource in Quantum Computing.
4. Estimate various Security Measures to protect the resource in Quantum Computing.
5. Execute various measures to protect the resources in Data Quantum Computing.
6. Review the Level of Security implemented in Quantum Computing to Prevent Unauthorized Access.
7. End.



S.No	Types of Attacks possible on Quantum Computing Technology before implementing the Security Measures	Percentage of vulnerability
1.	Shor's Algorithm and Cryptography	5.5
2.	Quantum-Safe Cryptography	6.3
3.	Data Security	8
4.	Block chain Security	7.2
5.	Quantum Security	9
Vulnerability after the Implementation of Proposed Security Measures		36

Table 2. Types of possible attacks on Quantum Computing after implementing the Security Measures



IV. CONCLUSION & FUTURE WORK

Even though several securities are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of Quantum Computing. Hackers / introduces are continuously making attempt to gain the unauthorized access of Quantum Computing using various attacks. As Quantum computing usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Quantum Computing several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

V.REFERENCE

[1] A.M.Turing. On computable numbers, with an application to the Entscheidung problem. In Proceedings of the London Mathematical Society, volume 42, pages 230–265, 1936. Correction, ibidem (vol. 43), pages 544–546.

[2] Y. Manin. Vychislimoe i nevychislimoe (computable and non-computable). Soviet Radio, pages 13–15, 1980. In Russian.

[3] Y. Manin. Classical computing, quantum computing, and Shor's factoring algorithm. quantph/9903008, 2 Mar 1999.

[4] R. Feynman. Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7):467–488, 1982.

[5] R. Feynman. Quantum mechanical computers. Optics News, 11:11–20, 1985.

[6] P. A. Benioff. Quantum mechanical Hamiltonian models of Turing machines. Journal of Statistical Physics, 29(3):515–546, 1982.

[7] D. Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum Turing machine. In Proceedings of the Royal Society of London, volume A400, pages 97–117, 1985.

[8] J. Preskill. Quantum computing 40 years later. In A. Hey, editor, Feynman Lectures on Computation. Taylor & Francis Group, second edition, 2022. arXiv:2106.10522.

[9] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. In Proceedings of the Royal Society of London, volume A439, pages 553–558, 1992.

[10] D. Simon. On the power of quantum computation. SIAM Journal on Computing, 26(5):1474– 1483, 1997. Earlier version in FOCS'94.

[11] E. Bernstein and U. Vazirani. Quantum complexity theory. SIAM Journal on Computing, 26(5):1411–1473, 1997. Earlier version in STOC'93.

[12] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5):1484–1509, 1997. Earlier version in FOCS'94. quant-ph/9508027.

[13] R. Rivets, A. Shamir, and L. Adelman. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21:120–126, 1978.

[14] S. Apes and R. de Wolf. Quantum speedup for graph scarification, cut approximation and Palladian solving. In Proceedings of 61st IEEE Annual Symposium on Foundations of Computer Science, pages 637–648, 2020. arXiv:1911.07306.

[15] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179, 1984.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Protection Consequence in Fog Computing

Y. Padmaja,
23CSC16, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
padmajayamanda4015@gmail.com

K.Krishna Prasanna,
23CSC11, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada,A.P,India
prasannakona2001@gmail.com

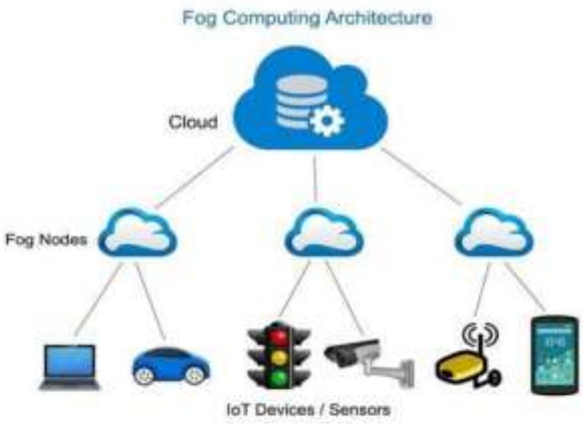
A.Sai Tejaswi.
23CSC18, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
saitetaswiavanigadda@gmail.com

ABSTRACT: In the Era of Burgeoning Data and The Internet of Things (Iot), The Limitations of Traditional Cloud Computing in Addressing Latency and Real-Time Processing Demands Have Become Apparent. This Article Investigates the Transformative Potential of Fog Computing as A Decentralized Computing Paradigm That Extends Cloud Capabilities to The Edge of The Network. A Detailed Examination of Fog Computing's Architecture Reveals Its Hierarchical Structure, Seamlessly Integrating Cloud Servers and Edge Devices to Enhance Computational Efficiency. We Delve into The Applications Across Diverse Industries, Emphasizing Its Role in Optimizing Latency sensitive Tasks and Improving Overall System Performance. Additionally, The Article Outlines Key Challenges and Explores Potential Solutions, Providing A Holistic View of The Current Landscape and Future Prospects of Fog Computing. As Businesses and Industries Increasingly Adopt Edge Computing Strategies, This Article Serves as A Vital Resource for Understanding the Nuanced Dynamics of Fog Computing and Its Pivotal Role in Shaping the Future of Distributed Computing.

KEYWORDS: Network, Security, Authentication.

I. INTRODUCTION

Cloud computing plays the leading role to provide on demand location-independent computing services in cloud data centers that may be quite distant from the user. However, with the advent and widespread adoption of cloud computing, many new dimensions have been introduced to adapt it to the needs of various computing paradigms. Multitier cloud computing, edge computing, mobile edge computing and more recently fog computing are among the complementary trends emerged to help optimize resource utilization and to meet application requirements [1]. Several substantial devices are linked at an unequalled speed from the existence of the IoT. The relaying of information is possible due to the lining together of the devices inclusive of sensors, smart meters, mobile phones, smart automobiles, radio-frequency identification tags, personal digital the associate editor coordinating the review of this manuscript and approving it for publication was Utku Kose. assistants, and different gadgets [2].



The broadening of IoT results in the production of enormous information (Big Data) that consumes large computing assets, cache memory, and transmission capability. Cisco expects that 50 billion devices will be associated with the Internet by 2020. The extension technology for IoT is Cloud Computing (CC). We intend our framework to be deployed and controlled by the central government of a country. Governments have access to the test results and can control such an integrated mobile-fog computing framework. Moreover, relying on a private entity to manage such a framework can limit the preservation of data privacy. Additionally, in this work, we primarily consider and focus on user data privacy issues. Regardless of building a standard and secure data processing framework, we do not discuss advanced security threats related to mobile, fog, and cloud layer as there are rich literature on existing security measures [3]. Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives (e.g. Operational costs, security policies resource exploitation) [4]. Fog networking consists of a control plane and a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, fog computing emphasizes proximity to end-users and client objectives [5]. Fog computing is a model in which data and processing are concentrated on devices at the edge of the network, rather than almost entirely in the cloud [6]. Cloud computing plays the leading role to provide on-demand location-independent computing services in cloud data centers that may be quite distant from the user Fog computing presents a new computing paradigm where computation capability, storage capacity, and networking services are placed at the edge and/or in the network, rather than in the cloud over the Internet [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in Fog Computing:

Risks in fog computing:

1. Security Concerns:

a. **Data Security:** Storing and processing data at the edge increases the risk of unauthorized access and data breaches [8].

b. **Device Vulnerabilities:** Edge devices may have limited security measures, making them susceptibleto attacks and compromises.

2. Reliability and Availability:

a. **Network Dependency:** Fog computing heavily relies on network connectivity. If the network fails or experiences delays, it can impact the availability and performance of services [9].

b. **Edge Device Reliability:** Edge devices might be less reliable than centralized cloud servers, leading to potential service disruptions.

3. Regulatory Compliance:

a. **Data Governance:** Different regions may have varying data protection and privacy regulations, posing challenges in ensuring compliance across fogcomputing environments [10].

4. Dynamic Nature of Edge Environments:

a. Topology Changes: The dynamic nature of edge environments, with devices connecting and disconnecting frequently, can make it challenging to maintain a stable and predictable computing environment [11].

5. Single Point of Failure:

a. Centralized Components: If certain centralized components within the fog architecture fail, it can lead to a single point of failure for multiple edge devices and services [12].

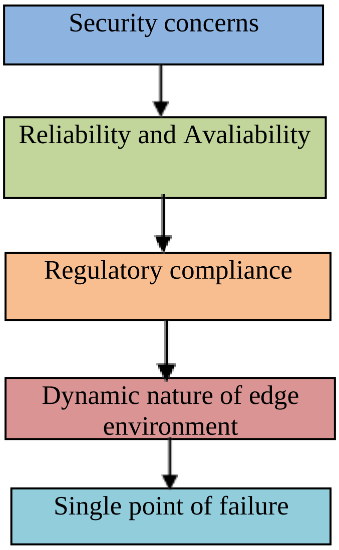

Security concerns
Reliability and Avaliability
Regulatory compliance
Dynamic nature of edge environment
Single point of failure

Fig.1.Various measures to Fog Computing

III. PROPOSED WORK

We propose, the following security methods to prevent threats on Fog Computing.

1. **Encryption:** Encrypt data in transit and at rest to protect it from unauthorized access. Use strong encryption algorithms to secure communication between fog devices and the cloud.
2. **Access Control:** Implement robust access control mechanisms to restrict unauthorized access to fog resources. This includes user authentication, authorization, and auditing. Only authorized users and devices should be allowed to access sensitive data and services.
3. **Network Security:** Deploy firewalls, intrusion detection and prevention systems, and secure gateways to monitor and filter network traffic. This helps in identifying and blocking potential security threats in real-time.
4. **Device Authentication:** Ensure that fog devices are properly authenticated before being allowed to participate in the fog network. Use secure protocols for device registration and authentication, and regularly update credentials to prevent unauthorized access.
5. **Secure APIs:** If fog devices communicate through APIs (Application Programming Interfaces), secure the APIs by using authentication tokens, encryption, and validating input to prevent attacks such as injection and manipulation of data.

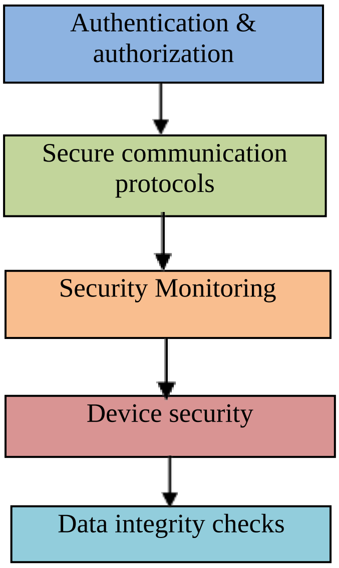

Authentication & authorization
Secure communication protocols
Security Monitoring
Device security
Data integrity checks

Fig.2.Various measures to Fog Computing

Algorithm:

1. Begin
2. Identify Potential Fog Computing Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End

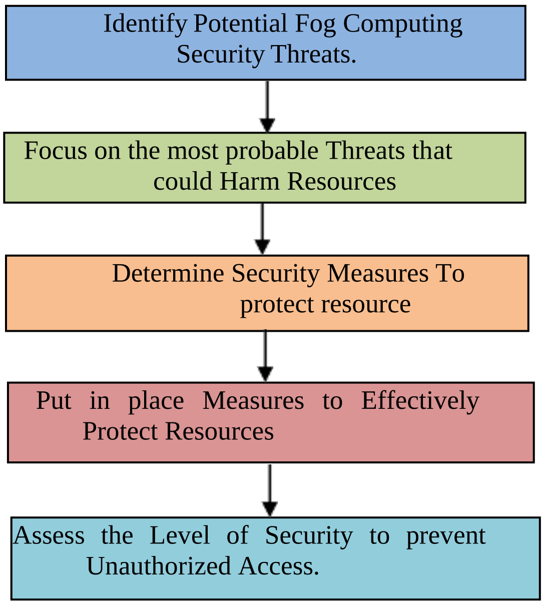

Identify Potential Fog Computing Security Threats.
Focus on the most probable Threats that could Harm Resources
Determine Security Measures To protect resource
Put in place Measures to Effectively Protect Resources
Assess the Level of Security to prevent Unauthorized Access.

Fig.4 Procedure to safeguard the resources of Fog Computing

IV. RESULT AND ANALYSIS

S. No	Types of attacks possible on Fog Computing before implementing the Security Risks	Percentage of Vulnerability
1	Security concerns	23
2	Reliability and Availability	19
3	Regulatory compliance	18
4	Dynamic nature of edge environment	20
5	Single point of failure	20
Vulnerability before the implementation of proposed Security Risks		100

Table 1. Types of Possible Attacks on Fog Computing before implementing the Security Risks

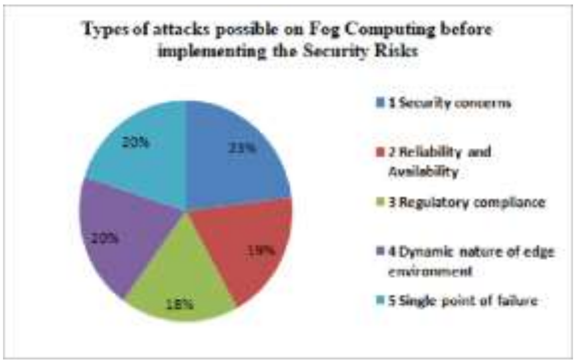


Fig.1.Risk before implementation of security Measures

S. No	Types of attacks possible onFog Computing after implementing the Security measures	Percentage of Vulnerability
1	Authentication and Authorization	7
2	Secure Communication Protocols	5
3	Security Monitoring	9
4	Device Security	4
5	Data Integrity Checks	5
Vulnerability after the implementation of proposed SecurityMeasures		30

Table 2. Types of Possible Attacks on Fog Computing after implementing the Security Measures

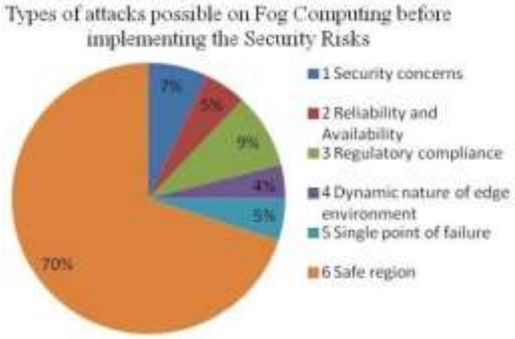


Fig.2.Enhancement of security after implementing security measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V.CONCLUSION AND FUTURE WORK

Effectively, fog computing is where a number of nodes receive information from devices, be they Internet of Things (IoT) devices or, for instance, factory production line sensors, and act upon it in real time. It is more powerful than edge computing alone and provides mission-critical analysis faster than cloud. The ability to conduct data analysis in real-time means faster alerts to potential failures and less likelihood of time lost in production process breakdowns, for example. Sometimes these fog nodes send summaries of data analysis to the cloud where it can be further analyzed to enable predictive decision making regarding various aspects of the device or systems, such as functionality and system health.

VI. REFERENCES

[1] Carla Mouradian," A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges" IEEE, 09 November 2017, DOI:10.1109/COMST.2017.2771153, ISSN:1553-877X

[2] C. M. D. Morais, D. Sadok, and J. Kelner, ''An IoT sensor and scenario survey for data researchers,'' J. Brazilian Comput. Soc., vol. 25, no. 1, pp. 1–17, Dec. 2019.

[3] R. Roman, J. Lopez and M. Mambo, " Mobile edge computing Fog et al.: A survey and analysis of security threats and challenges ", Future Gener. Comput. Syst., vol. 78, pp. 680-698, 2018.

[4] Forti, Stefano; Ferrari, Gian-Luigi; Brogi, Antonio (January 2020). "Secure Cloud-Edge Deployments, with Trust". Future Generation Computer Systems. 102: 775–788. arXiv:1901.05347. doi: 10.1016/j.future.2019.08.020

[5] Forti, Stefano; Ferrari, Gian-Luigi; Brogi, Antonio (January 2020). "Secure Cloud-Edge Deployments, with Trust". Future Generation Computer Systems. 102: 775–788. arXiv:1901.05347. doi: 10.1016/j.future.2019.08.020

[6] E. Riedel, G. A. Gibson and C. Faloutsos, "Active storage for large-scale data mining and multimedia", Proceedings of the 24rd International Conference on Very Large Data Bases ser. VLDB '98, pp. 62-73, 1998 DOI: 10.1109/FMEC.2017.7946412.

[7] J.-M. Kang, H. Bannazadeh, H. Rahimi, T. Lin, M. Faraji andA.Leon-Garcia, "Software-defined infrastructure and the future central office", Proc. IEEE Int.Conf. Commun. Workshops(ICC),pp.225229,Jun2013; DOI:10.1109/ACCESS.2020.2983253

[8] P. Hu, S. Dhelim, H. Ning, and T. Qiu, ''Survey on fog computing: Architecture, key technologies, applications and open issues,'' J. Netw. Comput. Appl., vol. 98, pp. 27–42, Nov. 2017.

[9] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, ''A comprehensive survey on fog computing: State-of-theart and research challenges,'' IEEE Commun.Surveys Tuts., vol. 20, no. 1, pp. 416–464, 1st Quart., 2018.

[10] B. Alturki, S. Reiff-Marganiec, C. Perera, and S. De, ''Exploring the effectiveness of service decomposition in fog computing architecture for the Internet of Things,'' IEEE Trans. Sustain. Comput., early access, Mar. 29, 2019, doi: 10.1109/TSUSC.2019.2907405.

[11] Sahmim S, Gharsellaoui H (2017) Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. Procedia Comput Sci 112:1516–1522.

[12] Stojmenovic I, Wen S (2014) The fog computing paradigm: Scenarios and security issues In: Computer Science and Information Systems (FedCSIS), 2014 Federated Conference On, 1–8.. IEEE.

Latest Research Trends in Virtual Reality Technologies

Ab.Sumiya Begum,
23CSC17,Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
abdulsumiyabegum@gmail.com

Prof.Srikanth Vemuru,
Dean-Faculty & Staff Affairs & Professor,
Dept. of Computer Science & Engineering,
Koneru Lakshmaih Education Foundation (Deemed to be University), Vaddeswaram, AP, India
deanfsa@kluniversity.in

N.Sai Kiran,
23CSC27, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
nanabalasaikiran123@gmail.com

ABSTRACT: Virtual Reality (VR) Is A Technology Which Allows A User to Interact with A Computer-Simulated Environment, Whether That Environment Is A Simulation of The Real World or An Imaginary World. It Is the Key to Experiencing, Feeling and Touching the Past, Present and The Future. It Is the Medium of Creating Our Own World, Our Own Customized Reality. It Could Range from Creating A Video Game to Having A Virtual Stroll Around the Universe, From Walking Through Our Own Dream House to Experiencing A Walk on An Alien Planet. With Virtual Reality, We Can Experience the Most Intimidating and Grueling Situations by Playing Safe and With A Learning Perspective. It Is Also Used for Military Training, Studies and Gaining Experience of The Thing That Might Not Be Possible in Reality. Now A Days, Most of The People Knows What Virtual Reality Is? But, In This Study We Will Have A Brief Introduction On VR, Some Important Portion of Its History, Terminology and Classes of VR System, Its Contribution in Modernization, Reviews and Analysis Of VR. While Moving Towards the Idea of Introducing VR In the Mass Media Sector.

Keywords: Virtual Reality, Humans, Computer Graphics, Computer Displays, Hardware, Airplanes

I. INTRODUCTION

Nowadays computer graphics is used in many domains of our life. At the end of the 20th century it is difficult to imagine an architect, engineer, or interior designer working without a graphics workstation. In the last years the stormy development of microprocessor technology brings faster and faster computers to the market. These machines are equipped with better and faster graphics boards and their prices fall down rapidly. It becomes possible even for an average user, to move into the world of computer graphics. This fascination with a new (ir)reality often starts with computer games and lasts forever. It allows to see the surrounding world in other dimension and to experience things that are not accessible in real life or even not yet created. Moreover, the world of three-dimensional graphics has neither borders nor constraints and can be created and manipulated by ourselves as we wish – we can enhance it by a fourth dimension: the dimension of our imagination [1]. Panoramic images can provide viewers with a 360 ∘ perspective of the scene, and create an immersive experience to viewers, which makes it plays an important role in virtual reality (VR) applications. In this paper, we propose a Multi-projection Fusion Attention Network (MFAN) to improve the accuracy of panoramic image quality assessment (PIQA). In particular, we propose to extract features from 2D plane images generated from multiple projection methods to overcome the distortions caused by a single projection [2]. The term "metaverse," in which the prefix "meta" refers to "far off" and the suffix "verse" refers to "universe," was initially coined in 1992 by Neal Stephenson in one of his science fiction novels, "Snow Crash"[3]. The concept of metaverses or virtual world goes beyond the commercial and entertainment, the idea in the future is to create true virtual societies, where digital users or avatars are our alter ego, thus tending to the creation of artificial societies in an environment digital [4].

Fig.1.Security and privacy risks of (VR)

The “serious” ways of using Metaverses seem to be the ones where a Metaverse acts as a facilitator for collaborative interaction or as a place of commerce. The topic of networked immersive collaborative environments is certainly not new. [5] The purpose of the virtual surface where it should gather and mirror actual-time global statistics and also inquire for immersion is to link the physical and digital worlds. Users’ physical inputs may be used to train artificial intelligence (AI) systems to provide client users with highly customized offerings. This technology offers an appropriate answer in the sphere of education and training by using its process. By using Metaverse extended reality, education sector will be changed drastically. [6] (VR) is a technology which allows a user to interact with a computer-simulated environment, whether that environment is a simulation of the real world or an imaginary world. It is the key to experiencing, feeling and touching the past, present and the future. It is the medium of creating our own world, our own customized reality [7]. The Vehicular Ad-Hoc Network, or VANET, is a technology that uses and moves cars as nodes in a network to create a mobile network. VANET is a special form of MANET (mobile ad hoc network). VANET makes every involving car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range [8]. Data communication between computers has brought about countless benefits to users, but the same information technologies have created a gap, a vulnerable space in the communication medium, where the data that's been exchanged or transferred, thereby causing threats to the data. Especially data on wireless networks are much exposed to threats since the network has been broadcasted unlike a wired network [9]. Data security in the past dealth with integrity, confidentiality and ensuring authorized usage of the data and the system. Less or no focus was placed on the reactive approach or measures to data security which is capable of responding properly to mitigate an attacker and avoid harm and also to prevent future attacks [10].

II. RELATED WORK

Risks in virtual reality:

Virtual reality (VR) and augmented reality (AR) offer plenty of amazing entertainment and educational opportunities, but despite the realistic and immersive depth of virtual worlds that exist in VR and AR, there are some real-world risks to using these technologies.One of the most widespreadexamples of the risks presented by virtual games and experiences came about after go pokemon was released in the summer of 2016. While it was not as immersive as full virtual reality, this AR game still managed to cause plenty ofinjuries, as people were so focused on the game that they weren't paying attention to their surroundings. Multiple car accidents, injuries like twisted ankles and bruised shins, and even robberies were reported as a result of people being too focused on the game.

1. Man-in-the-middle-attacks

Network attackers can listen in on the communications between the AR browser and the AR provider, AR channelowners, and third-party servers. This can lead to man-in- the-middle attacks.

2. Ransomware

Hackers may gain access to a user's augmented reality device and record their behavior and interactions in the AR environment. Later, they may threaten to release these recordings publicly unless the user pays a ransom. This could be embarrassing or distressing for individuals who do not want to see their gaming and other AR interactions made public.

3. Physical damage

One of the most significant AR security vulnerabilities for wearable AR devices is physical damage. Some variables are more durable than others, but all devices have physical vulnerabilities. Keeping them functional and secure – for example, by not letting someone walk off with a headset that can be easily lost or stolen – is an essential aspect of safety.

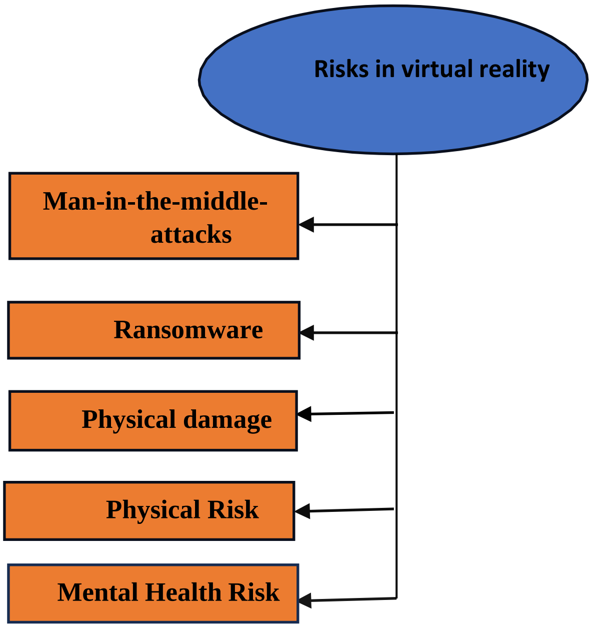


Fig.2.Various Risks to virtual reality

4. Physical Risk

Since a VR headset covers the eyes, users may fall, trip over or bump into objects, or lose their balance because they can't see their real-world environment. Users may also experience eye strain, which can lead to headaches. People who use VR headsets should first make sure that their play area is free of potential hazards. They should also reduce the amount of time they play to limit eye strain.

5. Mental Health Risk

Overstimulation, panic attacks, addiction, and a strong sense of fear and anxiety stemming from especially violentgames can come about due to the fact that these virtual environments feel real.

III. PROPOSED WORK

We propose the following security methods to safeguard the Virtual Reality from various security attacks.

Tips: How to stay safe when using virtual reality systems

a) Keep your device up to date and apply firmware updates and security patches as they become available
b) Keep your application software up to date.
c) Consider using a VPN when online.
d) Always use caution when installing applicationsfrom unknown sources.
e) Be careful when disclosing personal information

ofany kind.

f) Be particularly cautious in new environments.
g) Take additional steps to verify the identity of other users you interact and share data with.

Algorithm:

```
1) Begin
2) Identify potential Virtual Reality Threats.
3) Focus on the Most probable Threats thatcould Harm Resources.
4) Determine Security Measures to ProtectResources.
5) Put in place Measures to Effectively protect Resources
6) End
```

IV. RESULT & ANALYSIS

S.NO	Types of attacks possible on Virtual Reality before implementing the security Risks	Percentage of Vulnerability
1	Man-in-the-middle-attacks	12
2	Ransomware	20
3	Physical damage	13
4	Physical Risk	15
5	Mental Health Risk	40
Vulnerability before the implementation of proposed security Risks		100

Table1. Types of possible Attacks on Virtual Reality before implementing the Security Risks

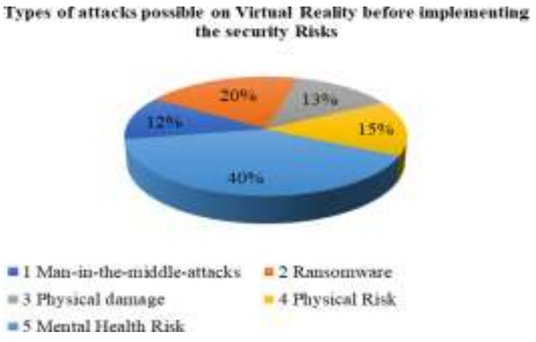


Fig.1.Risk before implementation of security Measures.

S.NO	Types of attacks possible on Virtual Reality before implementing the security Risks	Percentage of Vulnerability
1	Man-in-the-middle-attacks	5
2	Ransomware	9
3	Physical damage	7
4	Physical Risk	7
5	Mental Health Risk	6
Vulnerability after the implementation of proposed security Measures		34

Table1. Types of possible Attacks on Virtual Reality after implementing the Security Measures

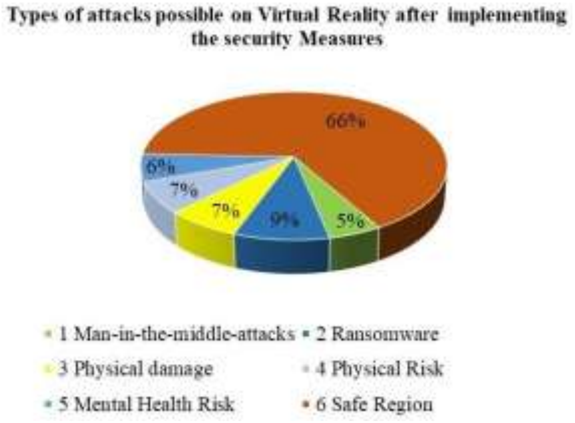


Fig.2.Risk after implementation of security Measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 34%.

V. CONCLUSION & FUTURE WORK

Even though several security measures are implemented using security protocols/firewalls which are unable to protect the vulnerabilities of VIRTUAL REALITY devices. Hackers/introduces are continuously making attempt to gain the unauthorized access of Virtual Reality devices using various attacks. As Virtual Reality devices usage has an effect on their usage. In order to protect the security and integrity of Virtual Reality devices several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Amanpreet Kaur et.al, “Virtual Reality: purpose of the metaverse”, IEEE, IEEE Xplore DOI:10.1109/ICDT57929.2023.10150886

[2] Huanyang Li et.al, “Virtual Reality: A Multi- Projection Fusion Attention Network for No- Reference and Full-

Reference Panoramic Image Quality Assessment”,IEEE,04-September- 2023,DOI:10.1109/LSP.2023.3310888

[3] N. Stephenson et.al, Snow crash: A novel. Spectra, 2003.

[4] J.Díaz et.al, “Virtual Reality: Virtual world as a resource for hybrid education", International Journal of Emerging Technologies in Learning (iJET), vol. 15, no. 15, pp. 94-109, 2020.

[5] I. Nikolaidis, “Virtual Reality: Networking the Metaverses," IEEE Network, vol. 21, no. 5, 2007,24 September 2007,DOI:10.1109/MNET.2007.4305173

[6] Khandaker Raiyan RAHMAN , “ Virtual Reality: Use of Metaverse Technology in Education Domain, https://doi.org/10.57019/jmv.1223704

[7] Sharmistha.M, “Virtual Reality: International Journal of Scientific” & Engineering Research, Volume 4, Issue 4, April-2013, ISSN 2229-5518.

[8] Kundalakesi Mathivanan, “Virtual Reality:A Research Paper on Vehicular Ad-Hoc Network”12- December-2018,IJSRD - International Journal for Scientific Research & Development,Vol. 5, ISSN (online): 2321-0613.

[9] Arif Sari, “Virtual Reality: Review of Data Security Techniques in Wireless Networks”,Vol.8 No.13, December 2015

[10] Mehmet Karay, “Virtual Reality: Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks”,30-December- 2015, http://www.trevormarshall.com/byte_articles/byte1. htm.

Block Chain Revolution Transforming Industries

CHAKKA LOKESH
23CSC19, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
chakkalokesh2002@gmail.com

BHARGAV GUJJALA,
23csc06, Student , M.Sc.(Computer Science)
Dept.of computer science,
P.B.Siddhartha College of Arts& Science,
Vijayawada, A.P, India
bhargavgujjala@gmail.com

DHANUNJAY MADDALI,
23CSC34, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
maddalidhanunjay111@gmail.com

ABSTRACT: Block Chain Technology Is an Advanced Database Mechanism That Allows Transparent Information Sharing Within A Business Network. A Block Chain Database Stores Data in Blocks That Are Linked Together in A Chain. Block Chain Technology Is More Advantageous in Supply Chain Management Since There Is A Constant Need to Record the Transaction History of Each Node/Party in The Block Chain Network. One Such Example is Storage of Blood Donation and Transfusion Data on Block Chain. As Multiple Parties Such as Blood Donor, Blood Bank and Hospital Are Involved, It Is Necessary to Keep the Part of Their Transactional Data (Such as Donor's Personal Data, Patient's Personal Data) As Confidential. Hence in This Paper, With the Intension to Provide More Data Confidentiality and Security, The Popular Data Encryption Algorithm 'Advanced Encryption Standard (AES)', A Symmetric Key Crypto- System Is Employed on Part of Blood-Chain Data Before Sending Transactions to The Ordering Service and Adding Blocks to The Ledger. Therefore, Only A Person Who Has Access to The Appropriate Key That Was Used to Create the Cipher Text Can Decrypt the Encrypted Data. In Addition, The Performance of The Transaction Using Different Parameters Such as Data Encryption/Decryption Speed, Storage Is Evaluated Using Hyper Ledger Caliper Tool.

KEYWORDS: Compliance, Accessing, Transaction, Security, Authentication.

I. INTRODUCTION

Now a days, the world is going through the new revolution which is known as digital revolution and it starts with the use of internet. With the usage of the internet, a new era of decentralization, no central authority, has been started, which will be supported by cryptography. Especially in the area of cryptography or digital cash, a lot of advances have been done by applying the scientific research. Earlier, the digital cash had been conceptualized with the implementation of central server which can prevent the double spending, privacy and having controlling power1-3. By implementing the advances of cryptography and decentralized network of computers, a new profound technology, which is known as Block chain, has been introduced. This emerging technology has the potential to change the life of society with new rules of spending and it will be the complete paradigm shift. The decentralized system, block chain, started a new era of global payments, corporate governance, democratic participation and functions of capital markets. The block chain, a novel technique, can ensure the security with privacy and consensus of all the players. In the present days, the block chain has to be understood by its definition, technique and usage along with the limitations. The block chain can be defined as a database which is distributed, shared, encrypted and it assists to develop as an irreversible and incorruptible public repository of information4-7. This technology permits, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority. In this technology, the security is ensured if no adversary wields a large fraction of the computational resource. The proposed technology, Block chain technology, has the potential to reduce the role of middleman who is one of the most important economic and regulatory actors in our society. It allows the people to transfer an exclusive piece of digital property or data to others, in a safe, secure, and incontrovertible manner. Block chain technology can create digital currencies that are not backed by any governmental body in case of demonetization. It can develop digital contracts or smart contracts, whose execution does not require any human intervention. It provides a market places in decentralized manner which can be operated free from the reach of regulation 8. It is also assisted by the decentralized platforms for communications and to monitor or spy those platforms will become more difficult in future days. It also generates the assets which are Internet-enabled assets that can be controlled just like digital property. Block chain is a world-shattering technology, and this technology will shift the balance of power from centralized authorities in various fields like business, finance, supply chain, voting, and intellectual property.

Fig.1 Block chain technology

II. RELATED WORK

1. **Security Concerns:** Despite being considered secure; block chain isn't immune to hacking. There have been instances of breaches and vulnerabilities, especially in less mature or poorly implemented systems.
2. **Regulatory Uncertainty:** The regulatory environment for block chain is evolving. Uncertain or restrictive regulations can impact the adoption and operation of block chain-based projects.
3. **Smart Contract Vulnerabilities:** Smart contracts, self-executing contracts with the terms directly written into code, can have coding errors or vulnerabilities, leading to unexpected outcomes or exploits.
4. **Scalability Issues:** Block chain networks, especially public ones, may face challenges in scaling to accommodate a growing number of transactions, causing delays and increased costs.
5. **Interoperability Challenges:** Different block chain platforms may have compatibility issues, hindering seamless communication and collaboration between different networks Risks of block chain

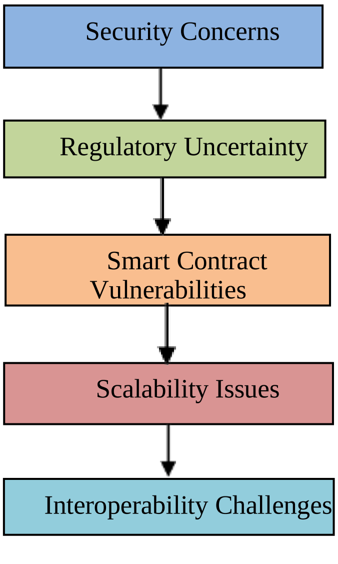
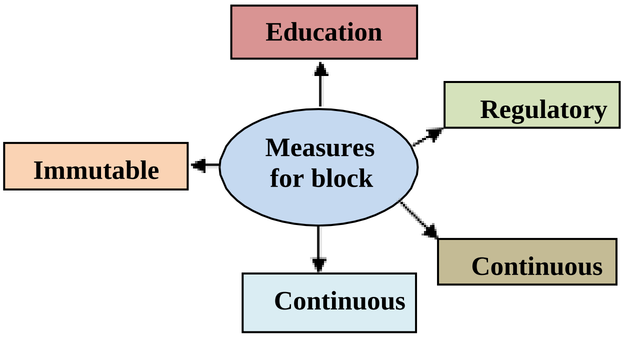


Fig.2. various security risks in block chain.

III. PROPOSED WORK

Measures for block chain

1. **Education and Training:** Provide education and training for developers and users on secure block chain practices. Awareness is keys to avoiding common pitfalls and security lapses.
2. **Regulatory Compliance:** Stay informed about and completely with relevant regulations. Adhering to legal standards can help in navigating the evolving regulatory landscape.
3. **Interoperability standards:** Encourage the development of interoperability standards to ensure smooth communication between different block chain networks, reducing the risk of vulnerabilities.
4. **Continuous Monitoring:** Implement real-time monitoring and anomaly detection tools to identify and respond promptly to any unusual activity or security breaches.
5. **Immutable Record Preservation:** While maintaining immutability is a core feature of block chain, it's important to ensure that erroneous or malicious transactions are not permanently recorded.



Algorithm:

1. Begin
2. Identify potential block chain threats.
3. Focus on the most probable threats that could harm resources.
4. Determine security measures to protect resources.
5. Put in place measures to effectively protect resources.
6. Assess the level of security to prevent unauthorized access.
7. End.

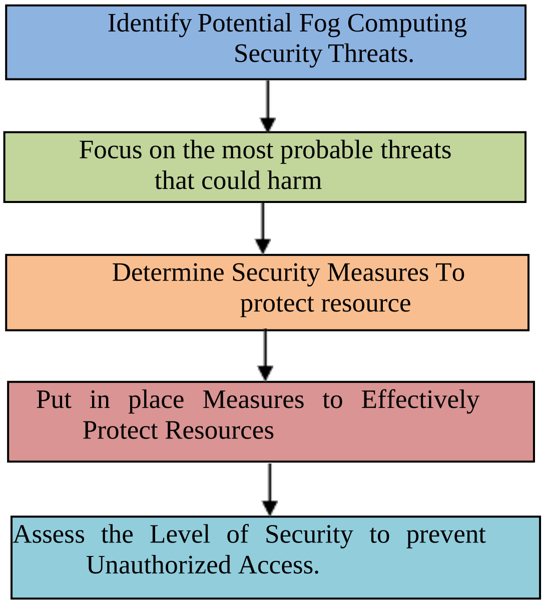

Identify Potential Fog Computing Security Threats.
Focus on the most probable threats that could harm
Determine Security Measures To protect resource
Put in place Measures to Effectively Protect Resources
Assess the Level of Security to prevent Unauthorized Access.

Fig.2. various security risks in block chain.

IV. RESULT & ANALYSIS

S.No	Types of attacks possible on block chain before implementing the security measures	Percentage of vulnerability
1	Security Concerns	24
2	Regulatory Uncertainty	18
3	Smart Contract Vulnerabilities	22
4	Scalability Issues	19
5	Interoperability Challenges	17
Vulnerability before the implementation of proposed security measures		100

Table 1. Types of possible attacks on block chain before implementing the security measures

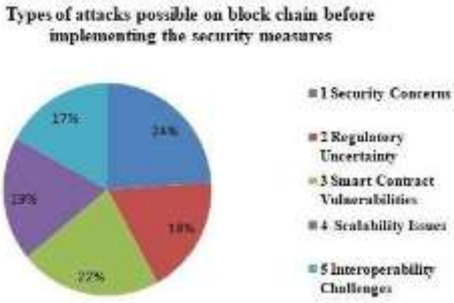


Fig.1 Types of attacks possible on block chain before implementing the security measures

S.No	Types of attacks possible on block chain after implementing the security measures	Percentage of vulnerability
1	Security Concerns	5
2	Regulatory Uncertainty	8
3	Smart Contract Vulnerabilities	9
4	Scalability Issues	3
5	Interoperability Challenges	5
Vulnerability after the implementation of proposed security measures		30

Table 2. Types of possible attacks on block chain after implementing the security measures

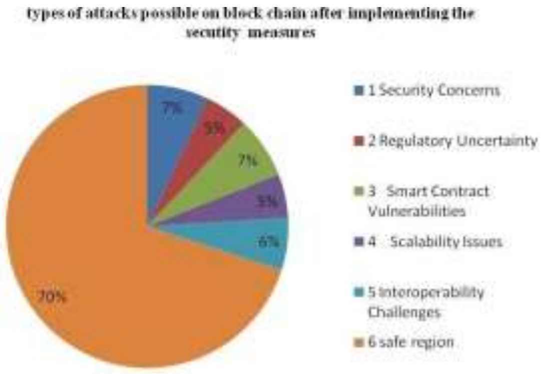


Fig.2 Types of attacks possible on block chain after implementing the security measures

After implement the security measures we have restricted most of the security risks from 100% to 35%.

V. CONCLUSION AND FUTURE WORK

Even though several security measures are implemented using several protocols/firewalls which are unable to protect the vulnerabilities of block chain. Hackers/introduces are continuously making attempt to gain the unauthorized access of block chain using various attacks as block chain usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of block chain several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] R.priya et.al,“block chain”,IEEE , 06 April 2023,DOI: 10.1109/ICNWC57852.2023.10127347 Electronic ISBN:979-8-3503-3600-9

I. [2].MENGYI XIE ET.AI, “DATA SECURITY BASED ON BLOCK CHAIN DIGITAL CURRENCY”, 25 OCTOBER 2020 , DOI:

10.1109/SMARTBLOCK52591.2020.00009 ELECTRONIC ISBN:978-1-6654-4073-8

II. [3]. RAMAN SINGH ET.AI, "BLOCK CHAIN-ENABLED END-TO-END ENCRYPTION FOR INSTANT MESSAGING APPLICATIONS" 17 JUNE 2022, DOI: 10.1109/WOWMOM54355.2022.00078 ELECTRONIC ISBN:978-1-6654-0876-9

[4] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] E. Karafiloski and A. Mishev, "Block chain solutions for big data challenges: A literature review," in Proc. IEEE EUROCON 17th Int. Conf. Smart Technol., 2017, pp. 763– 768.

[6] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure block chain-based data trading ecosystem," IEEE Trans. Inf. Forensics Secure., vol. 15, pp. 725–737, Jul. 2019.

[7] T. McGhin, K. R. Choo, C. Z. Liu, and D. He, "Block chain in healthcare applications: Research challenges and opportunities," J. Network Computer Appl., vol. 135, pp. 62–75, 2019.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using block chain for medical data access and permission management," in Proc. IEEE 2nd Int. Conf. Open Big Data, 2016, pp. 25–30. [9] F. Tian, "An agri-food supply chain traceability system for china based on RFID & block chain technology," in Proc. IEEE 13th Int. Conf. Service Syst. Service Manage., 2016, pp. 1–6.

[10] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed block chain cloud architecture for It," IEEE Access, vol. 6, pp. 115–124, 2017.

[11] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Block chain applications for industry 4.0 and industrial IoT: A review," IEEE Access, vol. 7, pp. 17 6935–17 6951, 2019.

[12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.
R. Choo, "P4- to-block chain: A secure block chain-enabled packet parser for software defined networking," Computer. Secure., vol. 88, p. 101629,2020

[13] A. Singh, R. M. Parizi, Q. Zhang, K. R. Choo, and A. Dehghantanha, "Block chain smart contracts formalization: Approaches and challenges to address vulnerabilities," Computer. Secure., vol. 88, p. 101654, 2020.

[14] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. R. Choo, "Side chain technologies in block chain networks: An examination and state-of-the-art review," J. Newt. Computer. Appl., vol. 149, p. 102471, 2020.

Revolutionizing Industries : The Impact of Robotics Technology

Ch.Udaya Bhavani,
23CSC21, Student,
M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts &Science
Vijayawada, A.P, India
chintaudayabhavani@gmail.com

Naveen Vijayakumar Watson,
Lecturer/IT College of Computer and Information Science,
University of Technology and Applied Sciences, CAS-Ibri campus,
naveen.kumar@utas.edu.om

Dr.B.Jaya Prakash,
Associate Professor,
Dept. of Business Adminstration,
P.B.Siddhartha College of Arts & Science, Vijayawada, AP, India
jayaprakash@pbsiddhartha.ac.in

ABSTRACT: Robots Are Automatic Equipment Integrating Advanced Technologies in Multiple Disciplines Such as Mechanics, Electronics, Control, Sensors, And Artificial Intelligence. Based on A Brief Introduction of the Development History of Robotics, This Paper Reviews the Classification of the Type of Robots, The Key Technologies Involved, And the Applications in Various Fields, Analyze the Development Trend of Robotics and Recent Research Hotspots, And Provide an Outlook on The Future Development of Robotics and Its Applications. It Also Presents Measures to Minimize These Attacks on Resources of Robotics Technologies. The Article Conducts A Thorough Examination of The Likelihood of Security Threats and Explores Various Ways to Minimize the Risks of Hacking, Providing Recommendations to Enhance Security. Robots Have BeenPart of Automation Systems for A Very Long Time, And in Public Perception, They Are Often Synonymous with Automation and Industrial Revolution Parse. Fueled by Industry 4.0 And Internet of Things (Iot) Concepts as Well AsBy New Software Technologies, The Field of Robotics in Industry Is Currently Undergoing A Revolution on Its Own.

KEYWORDS: Robotics, Security, Authentication Mechanisms, Robust Encryption, Boot Procedures.

I. INTRODUCTION

The industrial robotics sector is one of the most quickly growing industrial divisions, pro-viding standardized technologies suitable for various automation processes. In ISO 8373:2012standard [1], an industrial robot is defined as an automatically controlled, reprogrammable, multipurpose manipulator, programmable in three or more axes, which can be stationary or mobile for use in industrial automation applications. However, the same standard creates an exception for wider implementation. It states that the robot's classification into industrial, service, or other types is undertaken according to its intended application. In this context and in a nutshell, the RPA tools correspond to a set of techniques that aim to improve the work by reducing the number of repetitive tasks, automating them [2]. In addition to the use of RPA, the complement with Artificial Intelligence (AI) - algorithms and techniques - allows to improve the precision of the execution of automated processes. Industry 4.0 reviews a set of technologies and sensors that allows an even greater advance in the processes and applications of automation of AI applications for organizational processes, contributing to a better performance and presenting new opportunities. Robotic Process Automation (RPA) is the automation of services tasks that reproduce the work that humans do [3]. The automation is done with the help of software robots or AI workers that are able to perform, accurately, repetitive tasks. The task instructions are set by the developer using some form of screen recording and defining variables. These tasks include actions like logging into applications, copying and pasting data, opening emails, filling forms, among others. Van der Aalst et al. [3] state that "RPA is an umbrella term for tools that operate on the user interface of other computer systems". The construction industry is one of the most important economic sectors across the world [4]. The spending in construction represents between the 9%– 15% of GDP in most countries and up to half of nation's investment can be allocated to the built environment [5].

II. RELATED WORK

Robotics Technology Risks:

Here are some risks in robotic technology. Here we discuss below.

1. **Increase in the rate of unemployment**
   Finally, the depth of the whole robot scenario is the concern surrounding the sharp increase in the rate of unemployment. While we do not deny that robots will boost economic development and open doors to newer job avenues, it is also true that the same robots will be the cause of a major wave of unemployment. Studies

have shown that approximately 20 million manufacturing jobs will get automated by the fall of 2030. And other shows that a total of 30% of all jobs will employ robots shortly. With such numbers, it's not surprising that many people feel anxious about the rise of robots. And the job security and the common people source of income was the most concerning part [6].

2. **Robots Are Expensive Robots Replace Humans**
   Fast, error less, efficient, accurate, and continuous working is possible if robots do the job. Businessman looks forward to maximizing profit in every possible way. Like for doing repetitive jobs, he prefers robots rather than men. But it is not possible to have robots all the time because the upfront cost is very high. Not every company has high investment potential to fulfill the need. To run the robots' expertise is a must, which again needs a skilled staff. That adds to the expense. The maintenance cost and the advance technical supports were way more expensive [7].
3. **Job Losses**
   The effect on jobs for employees is one of the main concerns surrounding the advent of Robotic Automation. The worry is that if a robot can work faster and more consistently, people might not even be required. These concerns are reasonable, yet they are not entirely true. The work was completed fast and the tasks completed without any delay and the accuracy was affecting the recruitment of the people [8].
4. **Initial investment costs**
   This is one of the main barriers that determine whether a corporation invests in Robotic Automation at present or not. A thorough business case must be developed to evaluate the opportunities and potential shortcomings of such heavy investment. However, the rewards can be significant in a short period of time. While it's not worth pose a threat to the business's stability for minimal returns, maintaining a steady cash flow in the meantime is essential. Generally, a structured repayment plan will be in place, making it easier to handle and manage finances [9].
5. **Emotionless**
   Robots can never interact as humans do. Robots lack empathy, and this is one of the disadvantages of employing robots to work. Certain tasks require personal human touch, such as artwork, animations, video making, and other creative domains. There are also economic disadvantages that the world will face. This can arise due to the breakdown of robotic machines employed at work. The need for large investments added with the maintenance of machines will lower the return on capital. Additionally, electronic waste generation can be a future concern. While on a societal level, there are chances for conflicts to flare up between people who debate their views on robots versus people. Mostly in the manufacturing industry the humans also interact with the robots many times it does cause injuries and life threat situations occur by this point [10].
6. **Maintenance and Security**
   The upfront cost is not the only aspect of making the robots expensive. The maintenance is also costly. You need an expert or engineer to fix the machine, which can be expensive. To this add the downtime cost. As computers are prone to cyber-attacks, so are robots. They don't have the senses to judge right or wrong. It can be hacked and programmed to malfunction. Cyber security problems associated with robots can be dangerous. The security risk was the most common and concerning factor in recent years the security breaches and data leakage can causes loss to the industry technically and financially [11].

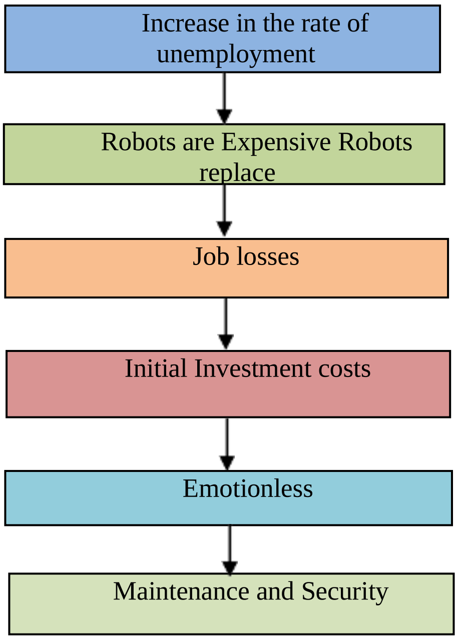

Increase in the rate of unemployment
Robots are Expensive Robots replace
Job losses
Initial Investment costs
Emotionless
Maintenance and Security

Fig.1.Various risks in Robotics Technology

III. PROPOSED WORK

We proposed the following security measures to safeguard the Robotics Technology from various security attacks

1. **Implement Robust Encryption:**
   Utilize advanced cryptographic protocols to safeguard communication channels and data transfers within the robotic systems. This ensures that sensitive information remains confidential and protected from unauthorized access. Like Other parties cannot access the database without the proper authentication.
2. **Deploy Intrusion Detection Systems (IDS):**
   Implement sophisticated IDS tools that can identify and respond to potential security threats in real-time. These systems can detect anomalies in the behavior of robotic devices, helping to mitigate risks associated with malicious activities. This will be so helpful to detect the unauthorized actions.

3. **Integrate Secure Authentication Mechanisms:** Employ strong authentication methods, such as biometrics or multi-factor authentication, to ensure that only authorized personnel can access and control the robotic systems. This prevents unauthorized individuals from tampering with the technology. Make sure to set the passwords strong and use all kind of alphabetics, number, special char etc.., for effective security.
4. **Regular Security Audits and Updates:** Conduct routine security audits to assess vulnerabilities in the robotic technology. Keep the software and firmware up- to-date with the latest security patches to address known vulnerabilities and enhance the overall resilience of the system. Install firewall security and test it frequently to keep it up-to-date and advance.
5. **Implement Secure Boot Procedures:** Utilize secure boot mechanisms to verify the integrity of the robotic systems software during the startup process. This prevents the execution of unauthorized or tampered code, reducing the risk of malicious actors gaining control over the robotics technology. Access own Wi-Fi networks do not connect the devices in other servers or other networks most of the time the outside servers and networks can causes bugs, data leakage and breaches.

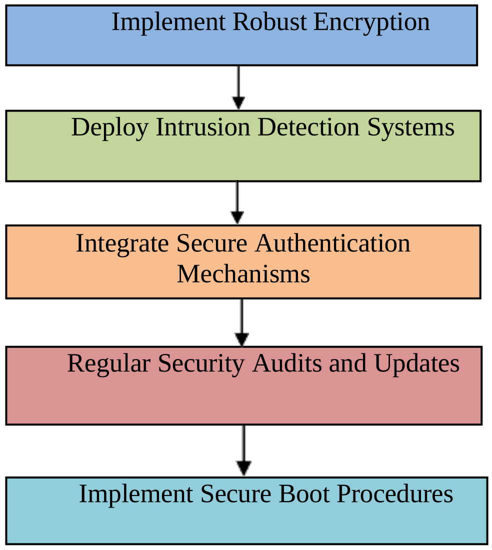

Implement Robust Encryption
Deploy Intrusion Detection Systems
Integrate Secure Authentication Mechanisms
Regular Security Audits and Updates
Implement Secure Boot Procedures

Fig.2. Various measures to reduce risks

Algorithm:

1. Begin
2. Identify potential Robotics Technology Security Threats
3. Focus on the most Probable threats that robotics harm resources
4. Determine security measures to protect resources
5. Put in place measures to effectively protect resources
6. Access the level of security to prevent unauthorized Access
7. End

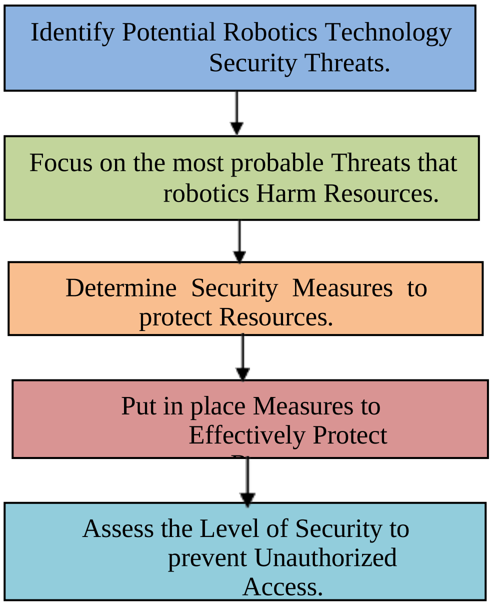

Identify Potential Robotics Technology Security Threats.
Focus on the most probable Threats that robotics Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect
Assess the Level of Security to prevent Unauthorized Access.

Fig. 3. Procedure to safeguard the resources of Robotics technology.

S.No	Types of Attacks possible on Robotics Technology before implementing the Security Measures	Percentage of Vulnerability
1	Increase in the rate of unemployment	20
2	Robots are Expensive Robots replace humans	15
3	Job losses	25
4	Initial investment costs	12
5	Emotionless	5.5
6	Maintenance and Security	22.5
Vulnerability before the implementation of Proposed Security Measures		100

Table 1. Types of possible Attack on robotics technology before implementing the Security Measures.

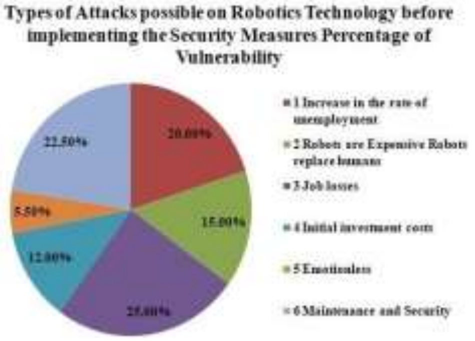


Fig .4. Vulnerability before implementing the Security Measures in Robotics

S.No	Types of Attacks possible on Robotics Technology after implementing the Security Measures	Percentage of Vulnerability
1	Increase in the rate of unemployment	5
2	Robots are Expensive Robots replace humans	5
3	Job losses	6
4	Initial investment costs	5
5	Emotionless	3
6	Maintenance and Security	3
Vulnerability after the implementation of Proposed Security Measures		27
Table 2. Types of possible Attack on robotics technology after implementing the Security Measures.		

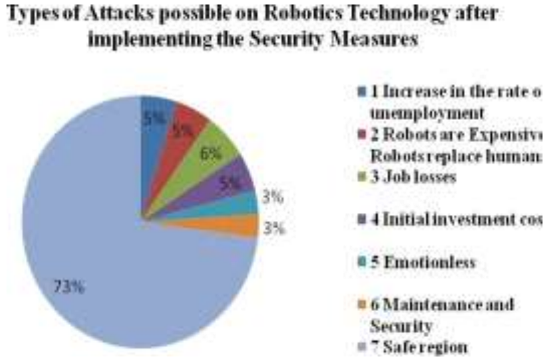


Fig. 5. Enhancement of Security after implementing Security Measures in Robotics Technology.

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

IV. CONCLUSION AND HARDWORK

Even though several security measures are implemented using security protocols /firewalls which are unable to protect the vulnerabilities of Robotics Technology. Hackers introduces are continuously making attempt to gain the unauthorized access of Robotics Technology using various attacks. As Robotics Technology has increased privacy and security challenges will have an effect on their usage in order to protect the security and integrity of Robotics Technology several new security measures, protocols and firewall needs to developed and effectively to challenge unauthorized access.

V. REFERENCE

[1] ISOISO8373:2012RobotsandRoboticDevicesVocabulary. Availableonline:https://www.iso.org/standard/55890.html(accessed on 7 April 2021)

[2] Aguirre, Santiago & Rodriguez, Alejandro. (2017). Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study. 65-71. DOI: 10.1007/978-3-319-66963-2_7.

[3] van der Aalst, W. M., Bichler, M., & Heinzl, A. (2018). Robotic Process Automation. Bus Inf Syst Eng 60, pp.269–272. https://doi.org/10.1007/s12599-018-0542-4

[4] R. Bogue What are the prospects for robots in the construction industry? Ind. Robot An Int. J., 45 (2018), pp. 1-6https://doi.org/10.1108/IR-11-2017-0194

[5] T.D. Oesterreich, F. Teuteberg Understanding the implications of digitization and automation in the context of Industry 4.0: a triangulation approach and elements of a research agenda for the construction industry Com. Ind., 83 (2016), pp. 121-139https://doi.org/10.1016/J.COMPIND.2016.09.006

[6] Mo UpaliSen et.al," Prediction of Unemployment using Machine Learning Approach", 2022 OITS International Conference on Information Technology (OCIT),DOI: 10.1109/OCIT56763.2022.00072

[7] Neil Sahota wt.al," When Robots Replace Human Managers: Introducing the Quantifiable Workplace", 29 July 2019, DOI: 10.1109/EMR.2019.2931654

[8] Radhamadhavan Madhavan et.al," The Impact of Robotics and Automation on Working Conditions and Employment", June 2018, DOI:10.1109/MRA.2018.2822058

[9] Munir Husein et.al," Evaluating Investment in Grid-Connected Microgrid Under Policy and Technology Risks", 29 November 2018, DOI: 10.23919/ICEMS.2018.8549393

[10] Miguel Castelo-Branco et.al," An Overview of Emotion in Artificial Intelligence", 16 March 2022, DOI: 10.1109/TAI.2022.3159614

[11] HongyiPu et.al," Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations", 25 July 2022, DOI: 10.1109/MNET.116.2200034

Protection Trails in 5G Network

G.Nandini
23CSC22, Student, M.Sc.(Computer Science), Dept. of Computer Science, P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
gundimedanandini2003@gmail.com

Bharat Kumar Reddy Gujavarti,
Founder & CEO,
Pragmatiq Systems Inc, Hyderabad
bharat@pragmatiq.in

K.B.S.M.D.S.Sai Prasanth
Ph.D. Scholar, IIT Madras Dept. of Electrical Engineering
kothuriprasanthkbs@gmail.com

ABSTRACT: 5G Is Expected to Bring Tremendous Advancement in Wireless Cellular Network by Providing Faster Speed, High Capacity and Low Latency. It Has Widely Been Adopted in Various Parts of The World and Is Expected to Bring A Noteworthy Revolution in Major Industries and Overall Economies. Although 5G Service Providers Are Promising Integrity, Confidentiality and Availability of Data, Still Security Is an Important Concern That Needs to Be Addressed. This Article Discusses Various Types of Attacks That Intruders or Hackers Can Carry Out to Gain Unauthorized Access Over Fog Computing Technologies. It Also Presents Measures to Minimize These Attacks on Resources of Fog Computing Technologies. The Article Conducts A Thorough Examination of The Likelihood of Security Threats and Explores Various Ways to Minimize The Risks Of Hacking, Providing Recommendations to Enhance Security.

KEYWORDS: Network Protection, Battery Life, Radiation.

I. INTRODUCTION

5G Technology stands for 5th generation mobile technology. 5G denote the next major phase of mobile telecommunication standards beyond the upcoming 4G standards. 5G technologies are offering the service in Product Engineering, Documentation, supporting electronic transactions, etc. As the customer become more and more aware of the mobile phone technology, he or she will look for a decent package all together including all the advanced features a cellular phone can have. [1]. The goal of a 5G based telecommunication network would ideally answer the challenges that a 4G model would present once it has entered widespread use. Wireless systems using orthogonal frequency division multiplexing (OFDM) with wide area coverage, high throughput at millimeter waves covering a frequency range of 30 GHz to 300 GHz, and enabling a 20 Mbps data rate to distances up to 2 km [2]. Several network operators use millimeter waves called FR2 in 5G terminology, for additional capacity and higher throughputs. Millimeter waves have a shorter range than the lower frequency microwaves, therefore the cells are of a smaller size. Millimeter waves also have more trouble passing through building walls and humans. Millimeter-wave antennas are smaller than the large antennas used in previous cellular networks [3].

How 5g Network Works:

Wireless networks are composed of cell sites divided into sectors that send data through radio waves. Fourth-generation (4G) Long-Term Evolution (LTE) wireless technology provides the foundation for 5G. Unlike 4G, which requires large, high-power cell towers to radiate signals over longer distances, 5G wireless signals are transmitted through large numbers of small cell stations located in places like light poles or building roofs [4]. The use of multiple small cells is necessary because the millimeter wave spectrum the band of spectrum between 30 and 300 gigahertz (GHz) that 5G relies on to generate high speeds can only travel over short distances and is subject to interference from weather and physical obstacles, like buildings or trees [5].

Evolution of 5G:

Cellular wireless networks have come a long way since the first 1G system was introduced in 1981, with a new mobile generation appearing approximately every 10 years. In the past 30 years, the mobile industry has transformed society through 4 or 5 generations of technology revolution and evolution, namely 1G, 2G, 3G, and 4G networking technologies.

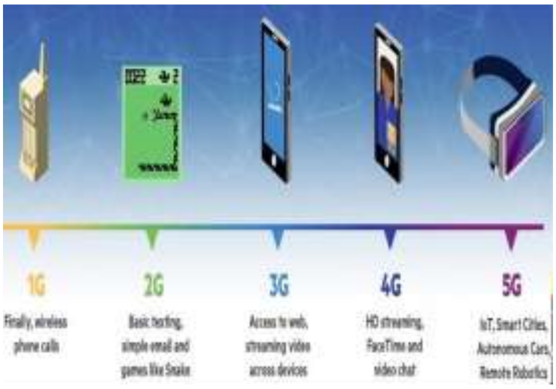

1G
Finally, wireless phone calls
2G
Basic texting, simple email and games like Snake
3G
Access to web, streaming video across devices
4G
HD streaming, FaceTime and video chat
5G
IoT, Smart Cities, Autonomous Cars, Remote Robotics

Fig.1. Evolution of 5G

How fast is 5G?

5G download speeds can currently reach upwards of 1,000 megabits per second (Mbps) or even up to 2.1 Gbps. To visualize this, a user could start a YouTube video in 1080p quality on a 5G device without it buffering. Downloading an app or an episode of a Netflix show, which may currently take up to a few minutes, can be completed in just a few seconds. Wirelessly streaming video in 4K also becomes much more viable. If on mm Wave, these examples would currently need to be within an unobstructed city block away from a 5G node; if not, the download speed would drop back down to 4G [6].

Utilization Of 5g Network:

The utilization of 5G network is worldwide and few of them are mentioned below:

1. Medical operations on board the ambulance helicopter, this scenario requires both higher peak data rata and low latency. It also assumes robust 5G communication link even in disaster areas.
2. New generation smart agriculture by using micro robots, this scenario shows a 5G application to smart agriculture by using 5G's capability of low power consumption.
3. Entertainment, watching of Ultra High-Definition movies in a hyper express train at extremely high speed. Enabling users' experience by Ultra high-definition 3D live video of sport events from sport player's viewpoints [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in 5G Network:

1. **Risks in 5G Network:**
   Network Protection: Networks, like their predecessors, are not immune to security threats. However, the risks are amplified due to the sheer volume of devices that will be connected and the sensitive nature of the data they will handle. Cyber security concerns range from data privacy and protection to potential threats to critical infrastructure. The decentralized nature of 5G networks, with more data being processed at the edge, also opens up new points of vulnerability. Telecom operators and device manufacturers will need to invest significantly in robust security measures to protect against these threats [8].
2. **Probable Health Effects:** The potential health effects of 5G are a topic of ongoing debate. Some experts have raised concerns about the impact of the higher frequency radio waves used by 5G on human health. However, the FDA, World Health Organization and other health organizations have stated that the levels of radiofrequency radiation to which people are exposed from 5G are below the limits set by international guidelines and are not expected to have health effects [9].
3. **Battery Life on cellular devices:** 5G networks offer faster speeds and lower latency, but these benefits come at the cost of higher power consumption. This could lead to faster battery drainage in 5G-enabled devices, particularly when downloading or streaming large amounts of data. Device manufacturers will need to find ways to improve battery life to ensure that users can enjoy the benefits of 5G without constantly worrying about their battery level. For the time being, companies like Samsung are advising customers to use the "Optimize battery usage" settings [10].
4. **Skill and Education Gap:** The deployment and management of 5G networks require a new set of skills. There is a need for professionals who understand not only telecommunications but also cloud computing, cyber security, AI, and IoT. This skills gap is a significant challenge and will require investment in education and training to overcome. There's plenty of buzz already generating around 5G-enabled Smartphone's and other devices. However, their availability will hinge on how expensive they are for manufacturers to make, as well as how quickly the network rolls out. Some carriers in the U.S., South Korea and Japan have already launched 5G pilots in select cities, and manufacturers have confirmed compatible mobile devices are coming in 2019. autonomous vehicle technology waiting on 5G deployment, as they would be driving blind without the super-fast network to communicate [10].
5. **Risk on Wildlife:** This absorption can increase from 3% to 370%, which will lead to a change in insect behaviors. Many reports have found out that electromagnetic waves and high frequencies can be harmful to animals and insects as their body temperature gets altered, and they lose their orientation ability. There are many studies that claim that wildlife gets affected while others deny, but the truth is till now, 5G exposures haven't been researched properly, so jumping to a conclusion is difficult. In that case, we need to have a proper study and then ponder upon the thought of adapting to a new technology. The main component of the 5G network that will affect the earth's ecosystems is the millimeter waves. These waves have been linked to many disturbances in the ecosystems of birds. Researchers observed that after exposure to radiation from a cell tower for just 5-30 min, the eggs of sparrows were disfigured [10].

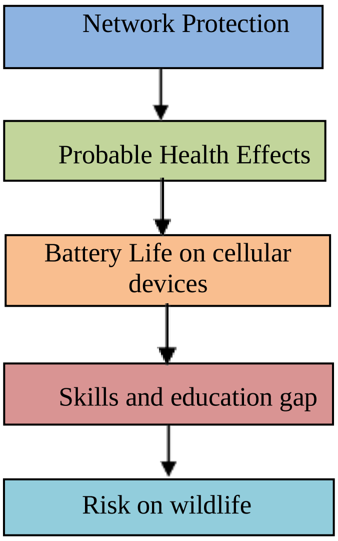


Fig.2. Various risks in 5G Network

III. PROPOSED WORK

We propose the following security methods to prevent threats on 5G Network:

1. **Improving Security:** To improve security issues on 5G networks, there are several measures that can be taken. some of the ways to overcome security challenges in the 5G world include:
   a. Establishing new open 5G security standards.
   b. Adopting APIs across vendors.
   c. Using agnostic management tools that can be centrally managed to see security events and orchestrate security policies.
2. **Network Segmentation and Multi-Factor Authentication:** Divide the 5G network into segments to limit the potential impact of a security breach. Segmentation helps contain threats and prevents unauthorized access to critical components. Enable multi-factor authentication for accessing critical systems and applications. MFA adds an extra layer of security by requiring users to provide multiple forms of identification before gaining access.
3. **Network Slicing:** Utilize network slicing to create virtual networks optimized for specific applications or services. Tailor network slices to meet the specific requirements of different use cases, such as IoT, enhanced mobile broadband, and ultra- reliable low-latency communication (URLLC).
4. **Improving signal strength:** 5G network, signal quality is measured as SINR. Increasing your SINR can have a dramatic impact on your connection speeds. The best way to improve SINR is to use a directional outdoor antenna, either connected to a signal booster or directly to an LTE.
5. **Increased Spectrum Availability:** Allocate additional frequency bands to increase overall bandwidth and capacity.

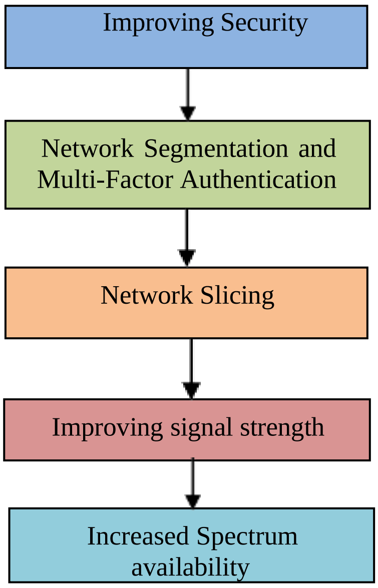

Improving Security
Network Segmentation and Multi-Factor Authentication
Network Slicing
Improving signal strength
Increased Spectrum availability

Fig.3. Various measures in 5G Network

Algorithm:

```
1. Begin
2. Identify Potential 5G Network Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End
```

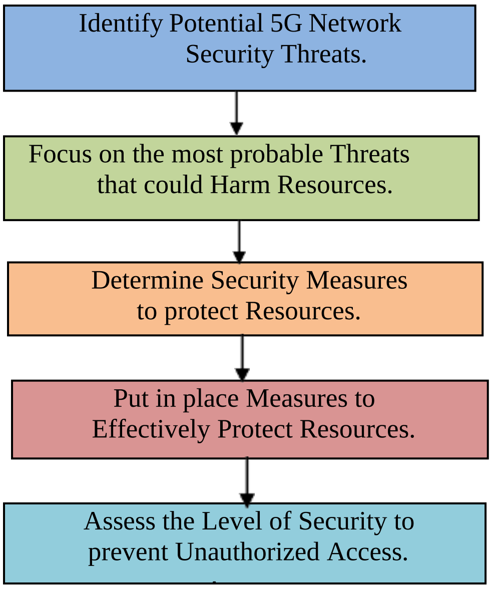

Identify Potential 5G Network Security Threats.
Focus on the most probable Threats that could Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 4. Procedure to safeguard the resources of 5G Network.

IV. RESULT AND ANALYSIS

S. No	Types of Attacks Possible on 5G Technology before implementing the security measures	Percentage of Vulnerability
1	Network Protection	22
2	Probable Health Effects	15
3	Battery Life on cellular Devices	18
4	Skills and Education Gap	20
5	Risk on Wildlife	25
Vulnerability before the implementation of Proposed Security Measures		100

Table 1. Types of possible Attacks on 5G Network before implementing the Security Measures

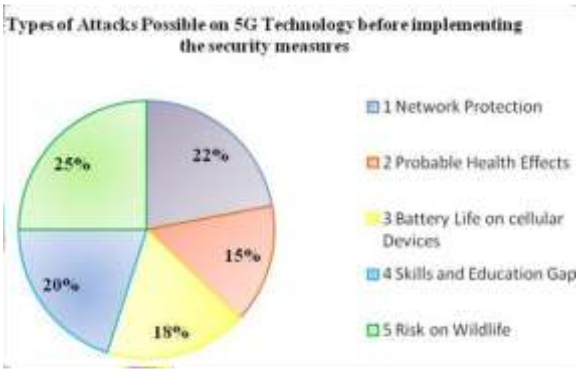


Fig.5. Risks before implementing the Security Measures

S. No	Types of Attacks Possible on 5G Technology after implementing the security measures	Percentage of Vulnerability
1	Network Protection	6
2	Probable Health Effects	5
3	Battery Life on cellular Devices	4
4	Skills and Education Gap	7
5	Risk on Wildlife	8
Vulnerability after the implementation of Proposed Security Measures		30
Table 2. Types of possible Attacks on 5G Network after implementing the Security Measures		

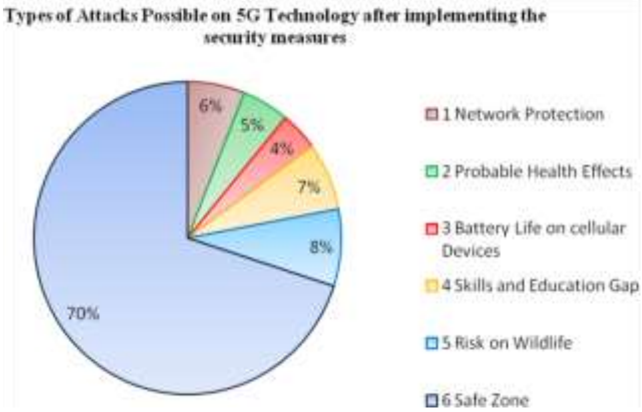


Fig.6. Risks after implementing the security Measures.

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION AND FUTURE WORK

In conclusion, the 5G network architecture is a complex and sophisticated system that combines advanced technologies, such as edge computing and network slicing, to provide high-speed, low-latency, and highly reliable communication for a wide range of applications and services. 5G is designed to have higher performance, the ability to manage thousands of devices, and extremely low latency. These attributes mean enterprises around the world are at least evaluating 5G for a broad variety of use cases.

VI. REFERENCES

[1] Neenu Welson et. al, “Introduction to 5G Wireless Technology”, IJERT, 19 May 2018, ISSN (Online) : 2278-0181, DOI: 10.17577/IJERTCONV4IS06018

[2] P. Schulz et al., “Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture” in IEEE Communications Magazine, 55(2): 70-78, 2017.

[3] Naik D C et. at, “Advancements and Challenges in5G Networks”, IEEE, 07-08 July 2023, Electronic, ISBN:979- 8-3503-4729-6, DOI:10.1109/ICSSES58299.2023.10201156.

[4] Mohsen Attaran, “The impact of 5G on the evolution of intelligent automation and industry digitization”, IEEE, 21-February-2021, DOI: 0.1007/s12652-020-02521-x.

[5] Mario Pons et. al, “Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties”, April 2023,10.3390/s23083876.

[6] Niranjan Lal et. al, “Prospects for Handling 5G Network Security”, Journal of Physics, 2021, DOI: 10.1088/1742-6596/1714/1/012052.

[7] Sunil Jain et. al, “5G Technology for healthcare and its health effects”, 16 Dec 2022, DOI: 10.4103/jfmpc.jfmpc_1426_22.

[8] Olimpjon Shurdi et.al, “5G Energy Efficiency Overview”, January 2021, European Scientific Journal, DOI:10.19044/esj. 2021.v17n3p315.

[9] Jianting Xue et. al, “Research on the impact of 5G technology on teaching behavior”, Journal of Physics, 2021, DOI: 10.1088/1742-6596/1955/1/012117.

[10] Adrew Wood et. al, “5G mobile networks and health”,6 March 2021, Doi: 0.1038/s41370-021-00297-6.

Navigating the Uncertainty : A Comprehensive Guide to AI Risk Management

G.RadhaKrishna,
23CSC23, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
sairadhakrishna1115@gmail.com

K.Kishore,
23CSC09, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
kishork1026@gmail.com

Ch.Nithin,
23CSC20, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
chigurupatinithin18@gmail.com

ABSTRACT: Artificial Intelligence (AI) Has Emerged as A Transformative Technology with The Potential to Revolutionize Various Aspects of Human Life. However, Alongside Its Promising Advancements, There Exists A Spectrum of Risks That Warrant Careful Consideration. This Abstract Provides an Overview of The Key Risks Associated with The Development, Deployment, And Integration of AI Systems.

KEYWORDS: Compliance, Artificial Intelligence (AI), Machine Learning (Ml).

I. INTRODUCTION

In the quest for sophistication, human beings have consistently developed and improved various technologies. The reason behind such practice is to ensure that they can come up with products that have the ability to provide an ease with how they carry out various methods [1]. Various activities have been taking place since humans came into existence, as they sought to ensure to have a chance of serving in different environments found. The practice would culminate in the early 1760s during the industrial revolution. During the period, various countries saw it possible to create different products for the masses to meet the demand for different products as a result of growing populations. Human beings have gone a notch higher since then, through the creation and adoption of artificial intelligence. The concept outlines the use of computer systems to perform tasks that usually need human intelligence. These are such as speech recognition, visual perception as well as decision- making [2]. The paper aims to outline various benefits and risks and misconception associated with artificial intelligence about transforming customer engagement. Artificial intelligence has been found to have tremendous advantages. One of the benefits is that it has increased the level of performance of physicians at hospital facilities. The situation acts in the interest of patients who are regarded as customers. The hospital staff can use computer systems specially developed to identify patients who are most at risk [3]. Such systems can precisely analyze the specific physiologic problems that various patients found at the hospital could be having and provide proper information about the patient who requires quick action. Through the process, the limited resources found at facilities could be used most efficiently to bring about the best outcomes, about ensuring they have the ability to meet the specific problems that patients may be going through to generally improve their quality of life [4]. Through such a process, computer systems are also able to aid in the process of decision making and save physicians the time they would have needed to consult widely on some of the health problems that the patients could be experiencing [5]. For instance, it has been used to determine the level of interaction of various drugs on patients to see if they have some antagonistic or synergistic effects on each other. Through the process of drug formulation, and clinical research, artificial intelligence has been used to analyze the vast amount of molecular information that relates to drug candidates to determine the general effects that it would have upon them[6]. In such a way, it would have the opportunity of ensuring they have the ability to identify the general implications of the specific drugs they put in the market. Pharmaceutical companies can apparently look into the different characteristics of the drugs they are developing. The process would enable them to put up various measures that would help them deal with the side-effects that could be associated with the drugs they develop [7]. Through the case, it ensures that such companies have the ability to provide the element of patient safety through the development of products that have a lesser chance of having adverse effects upon them. Artificial Intelligence also has a lot of importance in business. It is mostly used in the area of logistics by shipping companies to ensure they have the ability to move various cargo they are dealing with in the most appropriate fashion. Through the proper installation of a computer system, it can direct and monitor the movement of thousands of cargo in various parts of the world, to the point that they have the ability to reach the desired destination in time and make the particular company involved in such a case quite competitive. An example of such companies is the Port Botany container terminal found in Sydney, Australia [8]. What the system puts in place can monitor various cargo that moves around to different destinations to ensure they have the ability to meet the needs of the different clients who could be in need of their products. The process aids in the proper movement of such products quite efficiently, given the fact that any problems that may be identified in the same could be dealt with in a way that would help ensure success. Through the use of artificial intelligence, logistics and shipping companies have the ability to identify any mishaps that could have happened in the supply chain for the purpose of increasing the chances of the best outcomes on some of the actions they would have put in place to achieve success [9].

II. RELATED WORK

Several Risks in Artificial Intelligence (AI):

1. Autonomous weapons:

AI programmed to do something dangerous, as is the case with autonomous weapons programmed to kill, is one-way AI can pose risks. It might even be plausible to expect that the nuclear arms race will be replaced with a global autonomous weapons race. Russia's president Vladimir Putin said: "Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with enormous opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world." Aside from being concerned that autonomous weapons might gain a "mind of their own, " a more imminent concern is the dangers autonomous weapons might have with an individual or government that doesn't value human life. Once deployed, they will likely be difficult to dismantle or combat.

2. Social manipulation:

Media through its autonomous-powered algorithms is very effective at target marketing. They know who we are, what we like and are incredibly good at surmising what we think. Investigations are still underway to determine the fault of Cambridge Analytical and others associated with the firm who used the data from 50 million Facebook users to try to sway the outcome of the 2016 U.S. Presidential election and the U.K.'s Brexit referendum, but if the accusations are correct, it illustrates AI's power for social manipulation. By spreading propaganda to individuals identified through algorithms and personal data, AI can target them and spread whatever information they like, in whatever format they will find most convincing-fact or fiction.

3. Invasion of privacy and social grading:

It is now possible to track and analyses an individual's every move online as well as when they are going about their daily business. Cameras are nearly everywhere, and facial recognition algorithms know who you are. In fact, this is the type of information that is going to power China's social credit system that is expected to give every one of its 1.4 billion citizens a personal score based on how they behave things such as do they jaywalk, do they smoke in non-smoking areas and how much time they spend playing video games. When Big Brother is watching you and then making decisions based on that intel, it's not only an invasion of privacy it can quickly turn to social oppression [10].

4. Misalignment between our goals and the machine's:

Part of what humans' value in AI-powered machines is their efficiency and effectiveness. But, if we aren't clear with the goals, we set for AI machines, it could be dangerous if a machine isn't armed with the same goals we have. For example, a command to "Get me to the airport as quickly as possible" might have dire consequences. Without specifying that the rules of the road must be respected because we value human life, a machine could quite effectively accomplish its goal of getting you to the airport as quickly as possible and do literally what you asked, but leave behind a trail of accidents.

5. Discrimination:

Since machines can collect, track and analyses so much about you, it's very possible for those machines to use that information against you. It's not hard to imagine an insurance company telling you you're not insurable based on the number of times you were caught on camera talking on your phone. An employer might withhold a job offer based on your "social credit score." Any powerful technology can be misused. Today, artificial intelligence is used for many good causes including to help us make better medical diagnoses, find new ways to cure cancer and make our cars safer. Unfortunately, as our AI capabilities expand, we will also see it being used for dangerous or malicious purposes. Since AI technology is advancing so rapidly, it is vital for us to start to debate the best ways for AI to develop positively while minimizing its destructive potential [11].

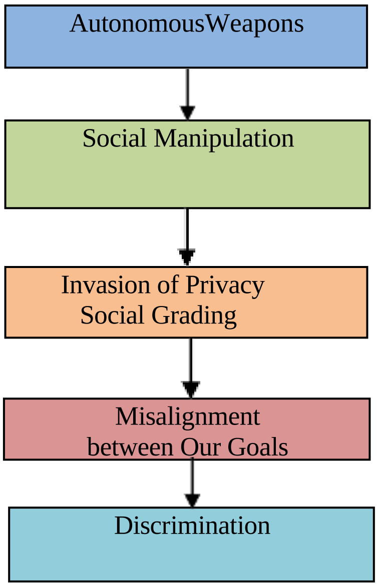


Fig.1.Several Risks in Artificial Intelligence (AI)

III. PROPOSED WORK

We propose the following security methods to safeguard the Artificial Intelligence for various security attacks.

Measures to Control the Risks of Artificial Intelligence (AI):

1. **Build integrity into your organization's AI from the design stage**

   "Just as employees need to be aligned with an organization's values, so too does AI," Atkinson and Mohamed write in VentureBeat. "Organizations should set the right tone from the top on how they will responsibly develop, deploy, evaluate, and secure AI consistent with their core values and a culture of integrity."

2. **Onboard AI as your organization would new employees and third-party vendors**
"As with humans, this due diligence process should be risk- based," the authors write. This will involve checking the "the equivalent of the AI's resume and transcript," such as "the quality, reliability, and validity of data sources used to train the AI," and the risks of using AI whose proprietary data is not available. It also includes checking "the equivalent of references to identify potential biases or safety concerns in the AI's past performance," as well as "deep background" checks, such as reviewing source code with the providers' consent in order to "root out any security or insider threat concerns."

3. **Ingrain AI into your organizational culture before deployment**
"Like other forms of intelligence, AI needs to understand the organization's code of conduct and applicable legal limits, and, then, it needs to adopt and retain them over time," Atkinson and Mohamed write. "AI also needs to be taught to report alleged wrongdoing by itself and others. Through AI risk and impact assessments, organizations can assess, among other things, the privacy, civil liberties, and civil rights implications for each new AI system."

4. **Manage, evaluate, and hold AI accountable**
Similar to how it might take a risk-based, probational approach to delving out responsibilities to new employees, your organization should do the same with AI. "Like humans, AI needs to be appropriately supervised, disciplined for abuse, rewarded for success, and able and willing to cooperate meaningfully in audits and investigations," the authors write. "Companies should routinely and regularly document an AI's performance, including any corrective actions taken to ensure it produced desired results."

5. **Keep AI safe from various dangers, such as physical harm and cyber threats, similar to what is done for employees:**
For especially risky or valuable AI systems, safety precautions may include insurance coverage, similar to the insurance that companies maintain for key executives, they write.

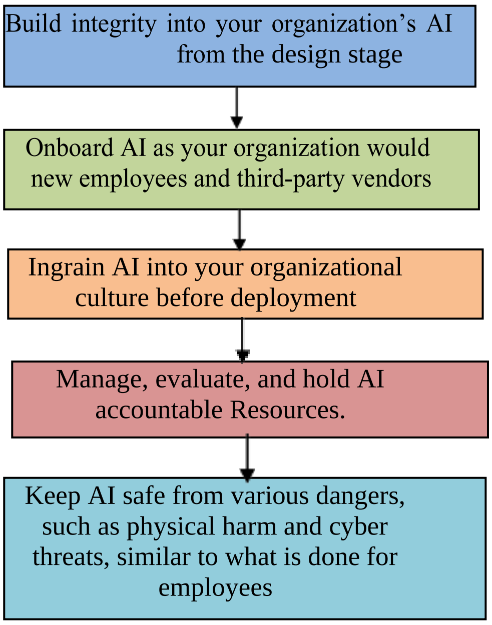

Build integrity into your organization's AI from the design stage
Onboard AI as your organization would new employees and third-party vendors
Ingrain AI into your organizational culture before deployment
Manage, evaluate, and hold AI accountable Resources.
Keep AI safe from various dangers, such as physical harm and cyber threats, similar to what is done for employees

Fig.2. Measures to Control the Risks of Artificial Intelligence (AI)

Alogorithm:

1. Begin
2. Identify the Potential risks in Artificial Intelligence (AI).
3. Concentrate on the main frequent risks that can damage the resource in Artificial Intelligence (AI).
4. Estimate various Security Measures to protect the resource in Artificial Intelligence (AI)
5. Execute various measures to protect the resources in Data Artificial Intelligence (AI).
6. Review the Level of Security implemented in artificial AI to Prevent Unauthorized Access.
7. End.

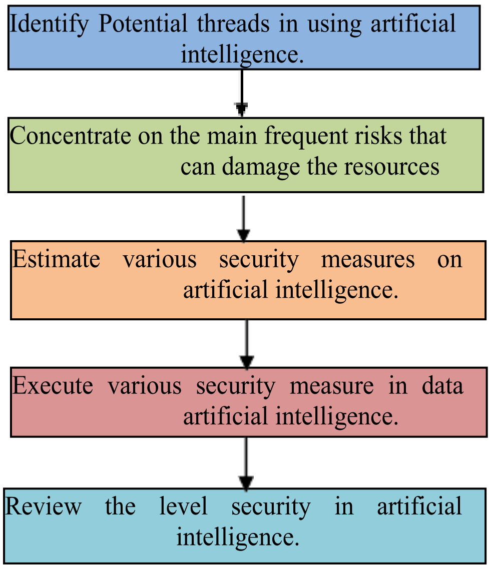

Identify Potential threads in using artificial intelligence.
Concentrate on the main frequent risks that can damage the resources
Estimate various security measures on artificial intelligence.
Execute various security measure in data artificial intelligence.
Review the level security in artificial intelligence.

Fig. 3. Procedure to safeguard the resources of securing finance

IV. RESULT & ANALYSIS

S.No	Types of Attacks on AI Applications Before Implementing the Security Measures	Percentage of Vulnerability
1	Autonomous weapons	18
2	Social manipulation	24
3	Invasion of privacy and social grading	20
4	Misalignment between our goals and the machine’s	19
5	Discrimination	19
Vulnerability before the implementation of proposed security measures		100
Table 1.Types of possible attacks on Artificial intelligence(AI) before implementing the security measures		

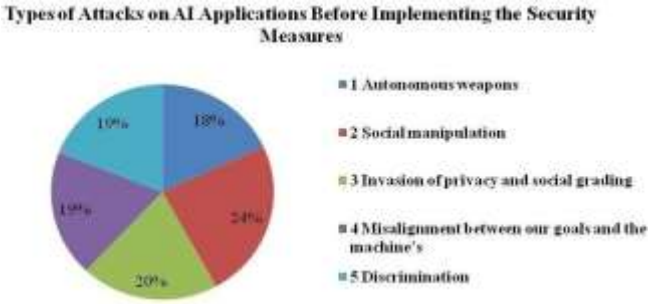


Fig.4.Vulnerability before the implementing of proposed security measures in Artificial Intelligence

S.No	Types of Attacks on AI Applications after Implementing the Security Measures	Percentage of Vulnerability
1	Autonomous weapons	6
2	Social manipulation	6
3	Invasion of privacy and social grading	6
4	Misalignment between our goals and the machine’s	4
5	Discrimination	4
Vulnerability after the implementation of proposed security measures		26
Table 2.Types of possible attacks on Artificial intelligence(AI) after implementing the security measures		

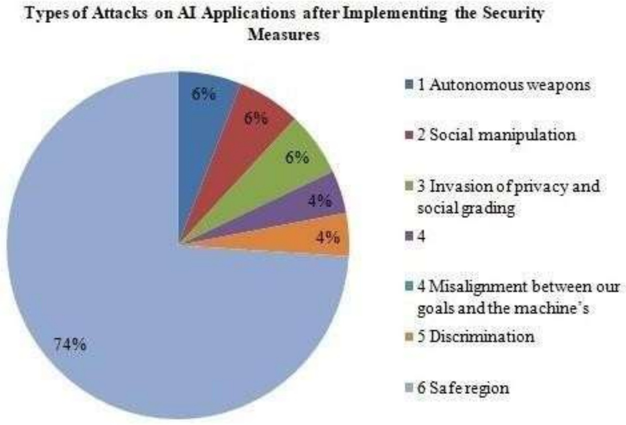


Fig.5.Vulnerability after the implementing of proposed security measures in Artificial Intelligence

After implement the security measures we have restricted most of the security risks from 100% to 35%.

V. CONCLUSION & FUTURE WORK

Even though several security measures are implemented using security protocols/firewalls which are unable to protect the vulnerabilities of Artificial Intelligence. Hackers/ introduces are continuously making attempt to gain the authorized access of Artificial Intelligence using various attacks. As Artificial Intelligence usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Artificial Intelligence several new security measures, protocols and firewalls need to be developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Hawking, Stephen, et al. "Stephen Hawking: \'Transcendence looks at the implications of artificial intelligence-but are we taking AI seriously enough?” The Independent 2014, pp. 31-36, 2014.
[2] M. Nadimpalli, “Artificial Intelligence - Consumers and Industry Impact”, Int J Econ Manag Sci, Vol. 6, pp. 429, 2017.
[3] Charniak, Eugene, et al. "Artificial intelligence programming", Psychology Press, vol. 27, 2014.
[4] Imran, Muhammad, et al. "AIDR: Artificial intelligence for disaster response." Proceedings of the 23rd International Conference on World Wide Web, ACM, pp. 67-82, 2014.
[5] Modgil, Sanjay, H. Prakken, "A general account of argumentation with preferences", Artificial Intelligence, vol. 195, pp. 361-397, 2013.
[6] Copeland, Jack "Artificial intelligence: A philosophical introduction" John Wiley & Sons, pp.81-84, 2015.
[7] Jones, M. Tim, "Artificial Intelligence: A Systems Approach: A Systems Approach. Jones & Bartlett Learning", pp. 107-109, 2015.

[8] Dreyfus, L. Hubert, "What Computers Can't Do: A Critique of Artificial Reason", vol. 20, pp. 51-55, 2016.
[9] Hovy, Eduard, R. Navigli, SP. Ponzetto, "Collaboratively built semi-structured content and Artificial Intelligence: The story so far", Artificial Intelligence vol. 194, pp. 2-27, 2013.
[10] Michalski, S. Ryszard, JG. Carbonell, TM. Mitchell, "Machine learning: An artificial intelligence approach", Springer Science & Business Media, pp.88-93, 2013.
[11] Boutilier, Craig, et al. "Optimal social choice functions: A utilitarian view", Artificial Intelligence, Vol. 227, pp. 190-213,2015.

Quantum Programming Paradigms : Shaping the Next Era of Software Development

V.Rama krishna,
23CSC25, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
ramakrishnamadi1020@gmail.com

P. Satya Naga Vara Prasad,
23CSC15, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
Satyaprasadpujari3699@gmail.com

G.Pavan,
23CSC03, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India
pavan.ganugupati97016@gmail.com

ABSTRACT: Quantum Computing, A Revolutionary Technology with The Potential to Transform Computational Capabilities, Brings Forth A Unique Set of Challenges and Risks. This Article Explores Ten Critical Risks Associated with Quantum Computing and Proposes A Comprehensive Set of Measurements to Control and Mitigate These Challenges. The Identified Risks Encompass Security Threats, Ethical Concerns, Economic Shifts, And Technical Limitations. The Proposed Measurements Include the Implementation of Robust Security Protocols, Continuous Research and Development, Education and Training Initiatives, International Collaboration, And the Promotion of Diversity Within the Quantum Computing Community. Additionally, The Article Emphasizes the Importance of Energy-Efficient Solutions, Effective Error Correction Strategies, Ethical Governance Frameworks, Open-Source Collaboration, And Regulatory Oversight. By Adopting These Measurements, The Quantum Computing Community Can Work Towards Responsible Development, Addressing Potential Pitfalls, And Fostering A Secure and Sustainable Quantum Ecosystem.

KEYWORDS: Malicious, Quantum Parallelism, Quantum Compilation, Security, Authentication.

I. INTRODUCTION

Quantum computing has been received numerous attentions in the last few decades, which is a framework based on Quantum Mechanism. Quantum mechanism is the basic framework or mathematical rule used to constitute the system of physics theory. When we reached twentieth century, a series of crises confused the scientists and some theories of physics were not valid anymore, such as ultraviolet catastrophe, which involves infinite energies. Nowadays, we have the ability to build a relatively complex quantum computer [1]. At bottom then, everything is quantum mechanical and, like Feynman in his visionary 1959 ‘Plenty of Room at the Bottom’ talk, we can certainly envisage storing bits of information on single atoms or electrons. However, these microscopic objects do not obey Newton's Laws of classical mechanics: instead, they evolve and interact according to the Schrodinger equation, the ‘Newton's Law’ of quantum mechanics.

Quantum Computing is a completely new model of computation based on the laws of quantum physics. It is not an improvement or extension of the current classical digital computing model that has been used for many years, but it is the first time in history that computing is branching. Significant resources are invested worldwide, and we are at the beginning of a new age of computation, developing programmable quantum systems towards universal quantum computers. Quantum computers promise to solve certain mathematical problems that are intractable to classical computers [2]. By using the physical phenomena of superposition, entanglement and interference, quantum computers can solve problems computationally hard for even the most advanced classical computers. Quantum entanglement creates strong correlations between qubit states leading to increased information in the combined system compared with the individual. Quantum Computing is the only way to enlarge the computational space and access this unique resource which cannot be mimicked by classical computing as it would require exponential resources. Quantum computing has become a reality. Quantum computers are available to everybody via cloud service or simulation. Toolkits are available that invite practitioners to start their own quantum software projects and thus get used to this novel technology [3]. In this article we evaluate technologies to help developers to start their own quantum software business. Practical guidance is provided from our own quantum technology projects. Quantum Computing (QC) has been a theoretical promise since the beginning of 1990‘s. A lot of research effort has been invested, especially in two areas. First, on the mathematics, logics and algorithms area. Second, quantum physicist and materials experts have been working on how to implement such a machine [4]. In the last years the importance of quantum computing has significantly increased due to both continuously shrinking of the size of silicon-based integrated circuits and the results in quantum algorithm development. The Moore's Law is well known today and it says that the number of transistors on integrated circuits doubles approximately every two years. Quantum computing offers a path forward by taking advantage of quantum mechanical properties. So, the rapid progress of computer science led to a corresponding evolution of computation from classical computation to quantum computation [5]. In general, quantum computers can be broadly classified into universal gate quantum computers and quantum annealers. The universal gate quantum computer/processor can be seen as a quantum counterpart to a classical general purpose microprocessor, where IBM (127 qubit) , Google (72 qubit) are in rapid pursuit of building faster and larger universal gate based quantum computers. On the other hand, the quantum annealers are akin to Application-Specific IC (ASIC), which can be used for solving a specific set of combinatorial optimization problems over discrete search space. However, the problems of interest in the domain of security primarily eyes the growth of universal quantum computers, which is not polynomials equivalent to quantum annealer.[6] Quantum computing has been a very active and promising area of research and, especially in the last years, of technology development. Since the physicist Richard Feynman proposed the idea of building a quantum computer to simulate quantum systems in the early 80’s, several quantum algorithms and quantum error correction techniques have been developed. By exploiting quantum phenomena such as superposition and entanglement, quantum computers promise to solve hard problems that are intractable for even the most powerful conventional supercomputers. In addition, remarkable progress has been made in quantum hardware based on different technologies such as superconducting circuits, trapped ions, silicon quantum dots, and topological qubits. A recent breakthrough in quantum computing has been the experimental demonstration of quantum supremacy using a superconducting quantum processor consisting of 53 qubits [7].

II. RELATED WORK

In this section, we exemplify various Security Risks in Quantum Computing:

Risks in Quantum Computing:

1. **Shor's Algorithm:** Quantum computers have the potential to efficiently solve certain mathematical problems, such as integer factorization, which is the basis of many cryptographic algorithms. This could render current encryption methods insecure [8].
2. **Quantum Key Distribution (QKD):** While QKD is proposed as a quantum-resistant cryptographic method, it is not immune to all potential attacks. Research is ongoing to ensure its practical security [9].
3. **Economic and Security Shifts:** The widespread adoption of quantum computing could lead to significant shifts in economic and geopolitical power, as countries or organizations that achieve quantum supremacy may gain a competitive advantage [10].
4. **Automation Impact:** Quantum computing ability to solve certain problems exponentially faster than classical computers could lead to job displacement in industries where classical computing is prevalent [11].
5. **Unintended Consequences:** As with any advanced technology, there may be unforeseen ethical consequences, such as the potential misuse of quantum computing for malicious purposes [12].

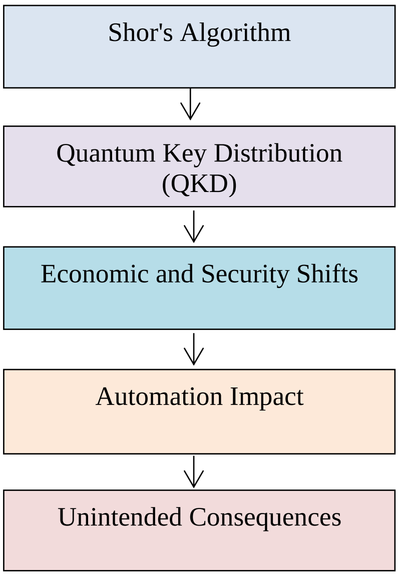


Fig. 1. various risks in quantum computing

III. PROPOSED WORK

We propose the following security methods to prevent threats on Quantum Computing.

1. **Research and Development**: Invest in ongoing research and development to stay ahead of potential security threats and vulnerabilities. Proactively address emerging risks through continuous innovation and collaboration with the quantum community.
2. **Education and Training:** Promote education and training programs to build a skilled workforce capable of addressing the unique challenges of quantum computing. Encourage awareness of ethical considerations and responsible use of the technology.

3. **International Collaboration:** Foster international collaboration and standardization efforts to ensure interoperability and a unified approach to quantum computing. Shared best practices and standards can help mitigate global risks and promote responsible development.
4. **Energy-Efficient Solutions:** Develop and implement energy-efficient quantum computing technologies to minimize the environmental impact and operational costs associated with large-scale quantum computing facilities.
5. **Error Correction Strategies:** Invest in research and development of effective error correction techniques to address the inherent challenges of quantum computers, such as decoherence and noise. Implement error correction protocols to enhance the reliability of quantum computations.

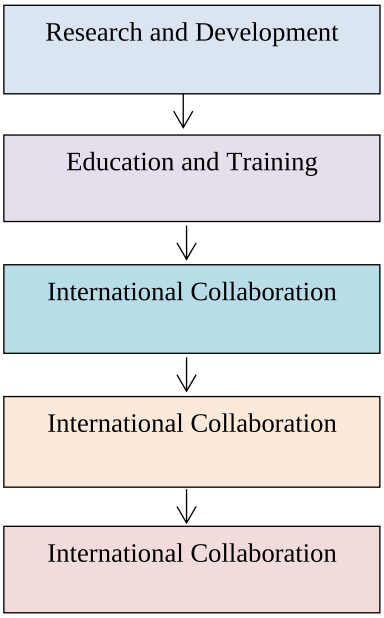

Research and Development
Education and Training
International Collaboration
International Collaboration
International Collaboration

Fig. 2. various measures in quantum computing

Algorithm:

1. Begin
2. Identify Potential Fog Computing Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End

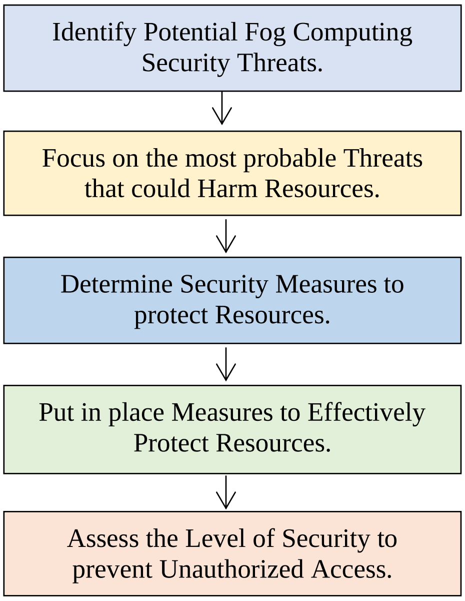

Identify Potential Fog Computing Security Threats.
Focus on the most probable Threats that could Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 4. Procedure to safeguard the resources of Fog Computing.

IV. RESULT & ANALYSIS

S. No	Types of Attacks possible on Quantum Computing Technology before implementing the Security Measures	Percentage of Vulnerability
1	Shor's Alogrithm	21
2	Quantum Key Distribution	19
3	Economic and Security Shifts	18
4	Automation Impact	22
5	Unintended Consequences	20
Vulnerability before the implementation of proposed Security Risks		100

Table 1. Types of Possible Attacks on Quantum Computing before implementing the Security Measures

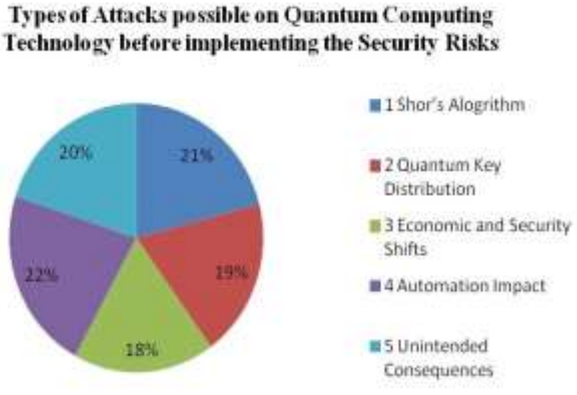


Fig.1. Risk before implementation of Quantum Computing

S. No	Types of Attacks possible on Quantum Computing Technology after implementing the Security Measures	Percentage of Vulnerability
1	Shor's Alogrithm	12
2	Quantum Key Distribution	5
3	Economic and Security Shifts	4
4	Automation Impact	6
5	Unintended Consequences	3
Vulnerability after the implementation of proposed Security Risks		30

Table 1. Types of Possible Attacks on Quantum Computing after implementing the Security Measures

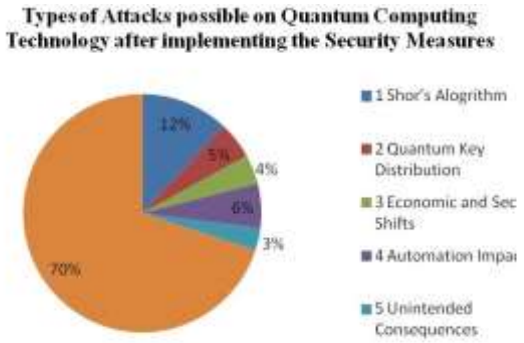


Fig.2. Risk before implementation of Quantum Computing

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols / firewalls which are unable to protect the vulnerabilities of Quantum Computing. Hackers/ introduces are continuously making attempts to gain the unauthorized access of Quantum Computing using various attacks. Quantum Computing devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Quantum Computing several new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Ziwei MENG et.al, "Review of Quantum Computing", 25 October 2020, DOI: 10.1109/ICICTA51737.2020.00051, Electronic ISBN:978-1-7281-8666-5.

[2] H.Riel et al.,Quantum Computing Technology",09 March 2022,DOI:10.1109/IEDMI19574.2021.9720538,Electronic ISBN: 978-1-6654-2572-8.

[3] Jose Luis Hevia et.al, "Quantum Computing", 20 August 2021, DOI: 10.1109/MS.2021.3087755, Electronic ISSN: 1937-4194.

[4] Rafael Sotelo et.al, "Quantum Computing What Why Who", 10 February 2020, DOI: 10.1109/CHILECON47746.2019.8988080, Electronic ISBN:978-1-7281-3185-6.

[5] Adina Barila et.al, "From Classical Computing to Quantum Computing", 15-17 May 2014, DOI: 10.1109/DAAS.2014.6842455, Electronic ISBN:978-1-4799-5094-2.

[6] Prasanna Ravi et.al, "Security and Quantum Computing an Overview", 08 September 2022, DOI: 10.1109/LATS57337.2022.9936966, Electronic ISBN:978-1-6654-5707-1.

[7] Carmen G. Almudever et.al, "Realizing Quantum Algorithms on Real Quantum Computing Devices", 09-13 March 2020, DOI: 10.23919/DATE48585.2020.9116240, Electronic ISBN:978-3-9819263-4-7.

[8] Aminah Albuainain et.al, "Experimental Implementation of Shor's Quantum Algorithm to Break RSA", 06 December 2022, DOI: 10.1109/CICN56167.2022.10008287, Electronic ISBN:978-1-6654-8771-9.

[9] V. Padamavathi et.al, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey", 28 February 2016, DOI: 10.1109/IACC.2016.109, Electronic ISBN:978-1-4673-8286-1.

[10] Mohammed Shuaib et.al, "Effect of Quantum computing on Blockchain-based Electronic Health Record Systems", 28 July 2022, DOI: 10.1109/ICSSA54161.2022.9870964 Electronic ISBN:978-1-6654-9981-1.

[11] Christina Petschnigg et.al, "Quantum Computation in Robotic Science and Applications", 24 May 2019, DOI: 10.1109/ICRA.2019.8793768, Electronic ISBN:978-1-5386-6027-0.

[12] Nouioua Tarek et.al, "The Quantum Computer and the Security of Information Systems", 22 September 2021, DOI: 10.1109/ICRAMI52622.2021.9585929, Electronic ISBN:978-1-6654-4171-1.

Understanding Human Perception in Virtual Environments

Ab.Sumiya Begum,
23CSC17, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
abdulsumiyabegum@gmail.com

N. Vijay Mohan,
23CSC26, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
vijaynallapu657@gmail.com

N.Sai kiran,
23CSC27, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
nanabalasaikiran123@gmail.com

ABSTRACT: Virtual Reality (VR), The Use of Computer Modeling and Simulation That Enables A Person to Interact with An Artificial Three-Dimensional (3-D) Visual or Other Sensory Environment. VR Applications Immerse the User in A Computer-Generated Environment That Simulates Reality Through the Use of Interactive Devices, Which Send and Receive Information and Are Worn as Goggles, Headsets, Gloves, Or Body Suits. In A Typical VR Format, A User Wearing A Helmet with A Stereoscopic Screen Views Animated Images of a Simulated Environment.

Keywords: Multimedia, Sight and Sound, Presence.

I. INTRODUCTION

“VR is a very high-end computer interface that evolves real time simulation and interface through numerous sensorial channels. These sensorial modalities are visual, aural, tangible, smell, taste and other senses” [1]. The first traces of virtual reality came from the short story "Pygmalion's Spectacles” in 1935by Stanley G. Weinbaum‟s is recognized as one of the first works of science fiction that see the sights of virtual reality. It describes a goggle-based virtual reality system with holographic demo of fictional experiences including aroma and feel.[2] Immersion is one of the main goals of virtual reality and when a virtual environment is created, it should be created with a view in the path of immersion. When immersion happens, the factual world can often be forgotten. Some characteristics of virtual reality are:

- A simulated environment
- Involves in computer-generated graphics.
- 3-dimensional.
- Involves in the use of human senses.
- exists in several different forms [3].

The first virtual reality system realized in hardware, not in concept. Ivan Sutherland constructs a device considered as the first Head Mounted Display (HMD), with appropriate head tracking. It supported a stereo view that was updated correctly according to the user’s head position and orientation [4]. In years 1960-1962 Morton Heilig created a multi-sensory simulator. A prerecorded film in color and stereo, was augmented by binaural sound, scent, wind and vibration experiences. This was the first approach to create a virtual reality system and it had all the features of such an environment, but it was not interactive [5].

The technological revolution has been permitting the use of new approaches in the teaching-learning process. One of the conductive technologies to the building of innovative tools for the education is the Virtual reality, which offers tridimensional computer environments with advanced forms of interaction that can provide more motivation to the learning process.[6] The traditional education system in India has long been in need of innovative approaches to engage students and make learning more effective. Virtual Reality (VR) technology has emerged as a promising tool for educational transformation. VR has the potential to provide immersive and interactive learning experiences, which can captivate students’ attention and enhance them understanding of complex subjects. This research article presents the results of a survey conducted among 25,000 students across various regions of India to understand their perceptions, preferences, and the potential future of VR in Indian schools. The survey aimed to answer critical questions:[7] The technological applications of VR have advanced to a point where they can be applied to an extensive range of fields and industries outside of just gaming or entertainment. Many have started to take advantage of VR in performing tasks that are hard to practice due to limited resources or the inherent risks and dangers associated with said tasks that can sometimes lead to catastrophic consequences. The greatest strength of VR is that it opens up opportunities for people to practice these tasks in a safe capacity while also being immersed enough for it to feel realistic and transferable to the real world and depict almost any situation accurately.[8] From infancy, a child learns through activity. With little control over its limbs, the process of learning about the world begins through exploration by reaching, touching, looking, smelling, and tasting whatever comes into its proximity. Through a combination of all the senses the child begins to associate different properties with different objects and through memorization is able to form distinct categories and concepts from the seemingly disparate and chaotic signals that it receives from the world. Even in maturity, perception and activity are crucial for learning.[9] The concept of VR was first introduced in the 1960s, with Morton's creation of the Telesphere Mask and the Sensorama The original technologies served the purpose of immersing the user in the video display around them, making them feel like they are a part of the video. The Ultimate display was an idea developed by Ivan Sutherland.[10]

II. RELATED WORK

What are the risks of virtual reality?

That VR offers a host of benefits—and has transformed how we think about technology—is well-known. However, VR is not without its downfalls. Here is our round-up of the top seven risks of VR.

1. **Cybersickness:** Cybersickness is a type of sickness that occurs when users spend extended periods in a virtual environment. Symptoms include nausea, disorientation, and headaches. This is caused by a disconnect between what users see in the virtual world and what their bodies are experiencing in the real world. To combat this, developers are working on creating more realistic virtual environments and designing shorter VR experiences.
2. **Data and privacy concerns:** As with any new technology, there are always data and privacy concerns. When it comes to VR, these concerns revolve around the fact that VR headsets collect a lot of data about their users. This data includes everything from biometric information to location data. While this data is collected to provide better VR experiences, there is a risk of leakage or non-consensual use of said data.
3. **Eye strain:** Another downside of VR is that it can cause eye strain. This is because VR headset displays are usually very close to users' eyes. To tackle this, developers are working on creating VR headset displays with higher resolutions and refresh rates.
4. **Isolation:** One of the risks of VR is isolation. This is because VR headsets cut users off from the outside world. This can lead to feelings of loneliness and anxiety. To combat this, developers are working on creating social VR experiences that allow users to interact with each other in the virtual world.
5. **Lack of content:** While there is a growing amount of VR content available, it is still quite behind when compared to other forms of entertainment, such as movies or video games. This lack of content is one of the main reasons why VR has yet to reach mass adoption.

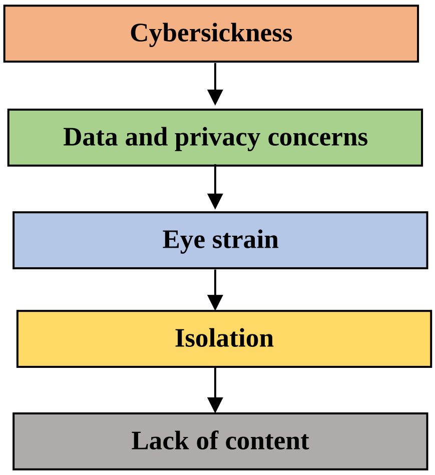


Fig. 2. various Risks in Virtual Reality

III. PROPOSED WORK

We propose the following security methods to safeguard the Virtual Reality from various security attacks.

Tips: How to stay safe when using virtual reality systems

1. **Create a Safe Physical Environment:** As you gear up for a VR training adventure, don't forget to ensure your physical surroundings are as safe as your virtual playground. VR immerses you so deeply that you might forget about your physical surroundings. Clear the area of potential obstacles and hazards to prevent real-world collisions.
2. **Mind the Cables**
   As much as wireless VR systems are making strides, many setups still involve cables. These cables can quickly become a tangled mess, leading to discomfort and potential hazards. Imagine trying to dodge virtual bullets while grappling with real-world cables – not the immersive experience you had in mind, right? To prevent such mishaps, invest in cable management solutions. These simple tools keep your cables organized, preventing tangling and tripping hazards, and ensuring your virtual adventures remain seamless and safe.
3. **Stay Hydrated and Take Breaks**
   In the captivating world of VR, time often seems to stand still. Hours can slip away while you're engrossed in your training. It's easy to forget about real-world necessities like hydration and rest. However, neglecting these needs can have a direct impact on your safety and well-being. Dehydration and eye strain can result from extended VR sessions. To counter this, maintain a water bottle nearby and remind yourself to take regular breaks. Stepping away from the virtual realm not only gives your eyes a rest but also prevents motion sickness, enhancing your overall VR experience.

4. **Adjust VR Settings Appropriately**
   One of the beauties of VR lies in its customization options. Just like adjusting the seat and mirrors in a car for a comfortable ride, VR allows you to tailor settings to suit your preferences. Take advantage of these features to optimize your experience. Adjust the field of view, brightness, and comfort settings to levels that feel right for you. Overly bright visuals can strain your eyes, while an incorrect field of view can lead to discomfort. By fine-tuning these settings, you're ensuring a personalized and safe experience that caters to your unique needs.
5. **Beware of Motion Sickness**
   Motion sickness is an unfortunate reality for some VR users, especially newcomers. Imagine taking a virtual roller coaster ride that leaves you feeling queasy – not exactly the thrill you were after. To mitigate the risk of motion sickness, it's crucial to ease into VR training gradually. Start with shorter sessions and gradually increase their length. This approach allows your body to acclimate to the virtual environment, building your tolerance over time. If you do start feeling dizzy or nauseous, don't push through it. Take a break and return to your training later. Remember, your safety and comfort are top priorities.

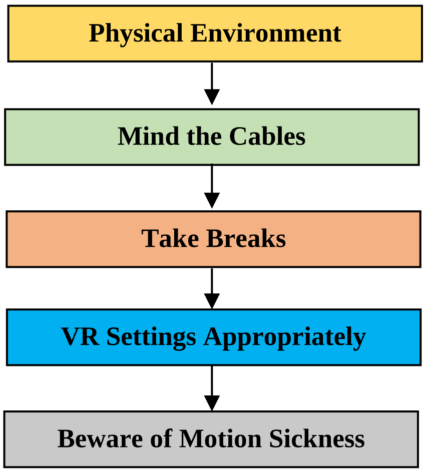


Fig. 3. various Security Threats in Virtual

Algorithm:

1. Begin
2. Identify potential Virtual Reality Threats.
3. Focus on the Most probable Threats that could Harm Resources.
4. Determine Security Measures to Protect Resources.
5. Put in place Measures to Effectively protect Resources
6. End

IV. RESULT & ANALYSYS

S.NO	Types of attacks possible on Virtual Reality before implementing the security Risks	Percentage of Vulnerability
1	Cybersickness	40
2	Data and privacy concerns	15
3	Eye strain	13
4	Isolation	20
5	Lack of content	12
Vulnerability before the implementation of proposed security Risks		100
Table1. Types of possible Attacks on Virtual Reality before implementing the Security Risks		

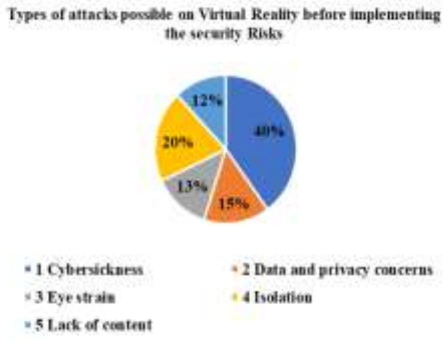


Fig.1.Risk before implementation of security Measures.

S.NO	Types of attacks possible on Virtual Reality After implementing the security Risks	Percentage of Vulnerability
1	Cybersickness	5
2	Data and privacy concerns	9
3	Eye strain	7
4	Isolation	7
5	Lack of content	6
Vulnerability after the implementation of proposed security Measures		34
Table1. Types of possible Attacks on Virtual Reality after implementing the Security Measures		

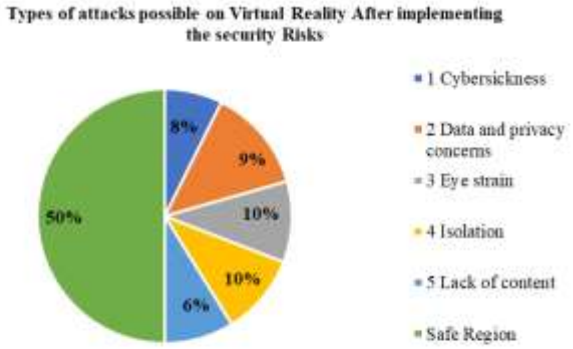


Fig.2.Risks after implementation of security Measures.

After implement the proposed security measures we have restricted most of the security threats from 100% to 34%.

V. CONCLUSION & FUTURE WORK

Even though several security measures are implemented using security protocols/firewalls which are unable to protect the vulnerabilities of VIRTUAL REALITY devices. Hackers/introduces are continuously making attempt to gain the unauthorized access of Virtual Reality devices using various attacks. As Virtual Reality devices usage has an effect on their usage. In order to protect the security and integrity of Virtual Reality devices several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] “Special study on virtual reality technology: virtual reality head-mounted display and interactive device” by sraSontisirkit. Asian institute of technology, school of engineering and technology, Thailand.
[2] Virtual reality society (2016) (information available at http://www.vrs.org.uk/virtual-reality-environments/)
[3] Virtual reality (2010) Wikipedia (Information available https://en.wikipedia.org/wiki/Virtual_reality)
[4] International Journal of Scientific & Engineering Research, Volume 4, Issue 4, April-2013 305 ISSN 2229-5518
[5] Tomasz mazuryk.e.l, December 1999, Institute of Computer Graphics Vienna University of Technology, Austria[mazuryk|gervautz]@cg.tuwien.ac.at http://www.cg.tuwien.ac.at
[6] Sandra Dutra Piovesan.e.l, ISBN: 978-989-8533-12-8 (C) 2012 IADIS
[7] KhritishS.e.l, 20Nov2023, SSRN: https://ssrn.com/abstract=4611167or http://dx.doi.org/10.2139/ssrn.4611167
[8] Arif Sari, “Virtual Reality: Review of Data Security Techniques in Wireless Networks”, Vol.8 No.13, December 2015
[9] Chris Christou.e.l, June 2010, DOI:10.4018/978-1-60566-940-3.ch012, book: Affective, Interactive and Cognitive Methods for E-Learning Design: Creating an Optimal Education Experience (pp.228-243)Edition: 1Chapter: 12Publisher: IGI Global Editors: Aimilia Tzanavari, Nicolas Tsapatsoulis
[10] Ayah Hmad.e. l, 2022 Sep 8, doi: 10.3390/ijerph191811278.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

VR Software and Content Development

N.Sai Kiran,
23CSC27,Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
Nanabalasaikiran123@gmail.com

Dr.J.Durga Prasad,
Asst. Professor, Dept of Business Adminstration,
P.B.Siddhartha College of Arts & Science, Vijayawada, AP, India
durgaprasad@pbsiddhartha.ac.in

Ab.Sumiya Begum,
23CSC17, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
abdulsumiyabegum@gmail.com

ABSTRACT: Virtual Reality (VR) Is A Powerful and Interactive Technology That Changes Our Life Unlike Any Other. Virtual Reality, Which Can Also Be Termed as Immersive Multimedia, Is the Art of Simulating A Physical Presence for The Audience in Places Both Real and Imaginary. It Usually Involves Two Senses Namely Sight and Sound. The Key Property That Distinguished VR From All Previous Media Types Is "Presence". Presence Is the Psychological Sense Of "Being There", Of Actually Being Immersed in And Surrounded by In the Environment. This Discussion Is an Attempt to Give an Overview of The Current State of Environment-Related VR, With an Emphasis on Live VR Experiences. The Technology, Art and Business of VR Are Evolving Rapidly. The Various Fields of VR Are Discussed to Get A Better View About It. The Next Development Based on Virtual Reality Is Augmented Reality.

KEYWORDS: Multimedia, Sight and Sound, Presence

I. INTRODUCTION

VR is a very high-end computer interface that evolves real time simulation and interface through numerous sensorial channels. These sensorial modalities are visual, aural, tangible, smell, taste and other senses. “The first traces of virtual reality came from the short story "Pygmalion's Spectacles" in 1935by Stanley G. Weinbaum‟s is recognized as one of the first works of science fiction that see the sights of virtual reality. It describes a goggle-based virtual reality system with holographic demo of fictional experiences including aroma and feel. A very important feature of virtual reality is the environment in which it takes place and must be vigilantly engineered to achieve a realistic experience. For example, if even the least of elements in a virtual reality environment is out of place, the entire experience can be smashed. For the it to be believable, it must achieve at least some height of immersion [1]. Immersion is one of the main goals of virtual reality and when a virtual environment is created, it should be created with a view in the path of immersion. When immersion happens, the factual world can often be forgotten. Some characteristics of virtual reality are:

- A simulated environment.
- Involves in computer-generated graphics
- 3-dimensional.
- Very interactive
- Involves in the use of human senses.
- Exists in several different forms [2]

Mobile applications are one of these new forms since smartphones and computer tablets are becoming a part of the student’s daily culture. The process of learning can be a complex task for the students since it requires a lot of effort from them, which is why they need the motivation to learn. Educational software for smartphones benefits the education process and makes it more interesting for students. Especially if it follows the computer game technology to render 3D graphics for the software and make it more amusing for the students while still deliver the necessary information.[3]

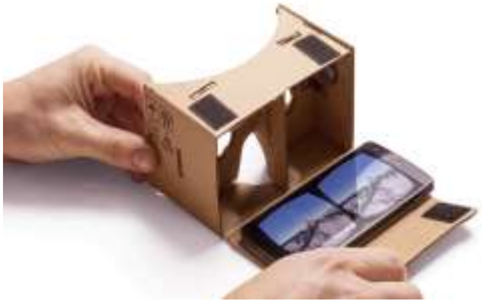


Fig 1. Google Cardboard

Currently there are many other mobile HMDs in the market following the Google Cardboard idea. Simple and cheap wireless HMDs that works in combination with an android or iOS devices and uses the stereoscopic display and the head tracking of the device. But Samsung had an idea of improving the wireless HMD experience that utilized mobile devices by introducing their own upgraded version building on top of the Cardboard idea. Samsung Gear VR is a wireless HMD developed by Oculus VR specifically for Samsung and their flagship phones, Galaxy Note 4 and Galaxy S6 devices.[4] Virtual Reality or VR allows a user to interact with a computer-generated three-dimensional model or virtual environment. This environment may be realistic, in the sense that it is familiar to us at a macroscopic scale, it may be realistic in the sense that it depicts the physical world as known to science but which is not usually observable, or it may be used to visualize a world that is entirely imaginary. As such, VR is broadly applicable, and has been applied to, many different areas of education including the sciences, archeology, history and architecture. [5] Virtual Reality (VR) is a three-dimensional digital environment which allows multiple degrees of freedom for the user to interact with the environment and engage in immersive interactions. Current foci in STEM Education disciplines require student to understand, manipulate, and incorporate complex and abstract ideas and observations. Some of the environments related to these ideas are impossible to replicate in educational settings.[6] Virtual Reality (VR) is a three-dimensional digital environment which allows multiple degrees of freedom for the user to interact with the environment and engage in immersive interactions. Current foci in STEM Education disciplines require student to understand, manipulate, and incorporate complex and abstract ideas and observations. Some of the environments related to these ideas are impossible to replicate in educational settings. [7] he user is immersed within the digital 3D world and is able to manipulate objects or perform actions within it. One way to access virtual reality is through a normal computer monitor screen, with early examples being the first-person shooter game, Quake and the Second Life virtual world.[8]

II. RELATED WORK

Augmented reality security and privacy issues

One of the biggest perceived dangers of augmented reality concerns privacy. A user’s privacy is at risk because AR technologies can see what the user is doing. AR collects a lot of information about who the user is and what they are doing to a much greater extent than, for example, social media networks or other forms of technology. This raises concerns and questions:

- If hackers gain access to a device, the potential loss of privacy is huge.
- How do AR companies use and secure the information they have gathered from users?
- Where do companies store augmented reality data – locally on the device or in the cloud? If the information is sent to a cloud, is it encrypted?
- Do AR companies share this data with third parties? If so, how do they use it?

1. **Unreliable content**
   AR browsers facilitate the augmentation process, but the content is created and delivered by third-party vendors and applications. This raises the question of unreliability as AR is a relatively new domain, and authenticated content generation and transmission mechanisms are still evolving. Sophisticated hackers could substitute a user’s AR for one of their own, misleading people or providing false information. Various cyber threats can make the content unreliable even if the source is authentic. These include spoofing, sniffing, and data manipulation.
2. **Social engineering**
   Given the potential unreliability of content, augmented reality systems can be an effective tool for deceiving users as part of social engineering attacks. For example, hackers could distort users' perception of reality through fake signs or displays to lead them into performing actions that benefit the hackers.
3. **Malware**
   AR hackers can embed malicious content into applications via advertising. Unsuspecting users may click on ads that lead to hostage websites or malware-infected AR servers that house unreliable visuals – undermining AR security.
4. **Stealing network credentials**
   Criminals may steal network credentials off wearable devices running Android. For retailers who use augmented reality and virtual reality shopping apps, hacking could be a cyber threat. Many customers already have their card details and mobile payment solutions already recorded in their user profiles. Hackers may gain access to these and deplete accounts silently since mobile payment is such a seamless procedure.
5. **Denial of service**
   Another potential AR security attack is denial of service. An example might involve users who rely on AR for work suddenly being cut off from the information stream they are receiving. This would be especially concerning for professionals using the technology to carry out tasks in critical situations, where not having access to information could have serious consequences. One example might be a surgeon suddenly losing access to vital real-time information on their AR glasses, or a driver suddenly losing sight of the road because their AR wind shield turns into a black screen.

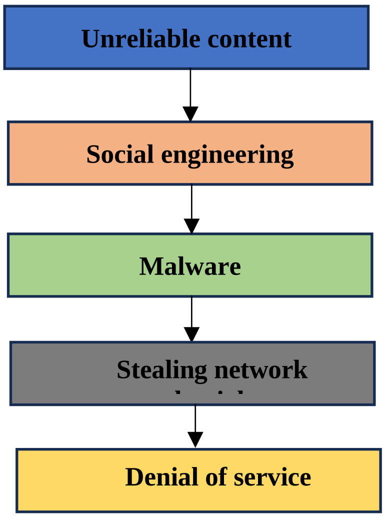


Fig.2.Various Security Threats in Virtual reality.

III. PROPOSED WORK

How to stay safe when using VIRTUAL REALITY

1. **Avoid the disclosing information that is too personal**
   Don't disclose any information that is too personal or doesn't need to be disclosed. It is one thing to set up an account with your email but don't set up your credit card unless you are explicitly purchasing something.
2. **Review seclusion policies**
   It is easy sometimes to skip over lengthy data privacy policies or terms and conditions. But it's worth trying to find out how the companies behind AR and VR platforms store your data and what they do with it. For example, are they sharing your data with third parties? What kind of data are they sharing and collecting?
3. **Benefits of Virtual Private Network**
   One way to keep your identity and data private on the web is by using a VPN service. If you need to disclose sensitive information, using a VPN can protect you from having that information compromised. Advanced encryption and an altered IP address work together to keep your identity and data private. With developments in AR and VR, the VPN model will likely expand within these tech realities.
4. **Keep firmware up to information**
   For your VR headsets it's vital to keep firmware up to date. As well as adding new features and improving existing ones, updates help to patch security flaws.
5. **Use extensive antivirus software**
   In general, the best way to stay safe online is by using a proactive cybersecurity solution. Such as Kaspersky Total Security which provides robust protection from various online threats. Such as, viruses, malware, ransomware, spyware, phishing, and other emerging internet security threats.

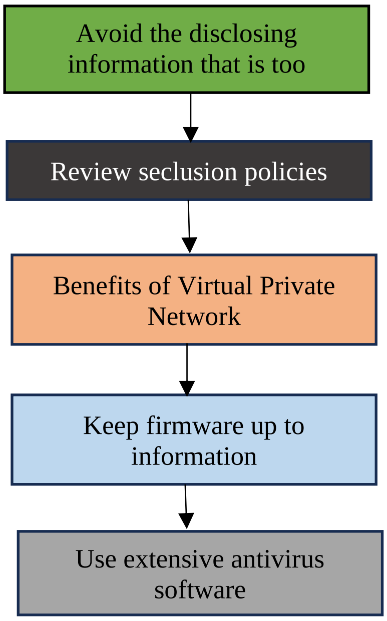

Avoid the disclosing information that is too
Review seclusion policies
Benefits of Virtual Private Network
Keep firmware up to information
Use extensive antivirus software

Fig.3.Various Security Threats in Virtual reality.

Algorithm:

```
1) Begin
2) Identify potential Virtual Reality Threats.
3) Focus on the Most probable Threats that could Harm Resources.
4) Determine Security Measures to Protect Resources.
5) Put in place Measures to Effectively protect Resources
6) End
```

IV. RESULT & ANALYSIS

S.NO	Types of attacks possible on Virtual Reality before implementing the security Risks	Percentage of Vulnerability
1	Unreliable content	17
2	Social engineering	19
3	Malware	23
4	Stealing network credentials	25
5	Denial of service	16
Vulnerability before the implementation of proposed security Risks		100

Table1. Types of possible Attacks on Virtual Reality before implementing the Security Risks

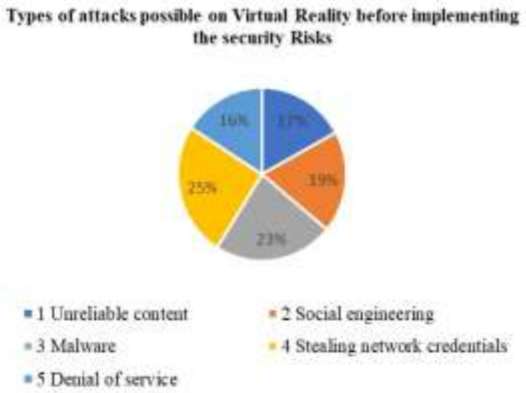


Fig.4.Risk before implementation of security Measures.

S.NO	Types of attacks possible on Virtual Reality After implementing the security Risks	Percentage of Vulnerability
1	Unreliable content	6
2	Social engineering	4
3	Malware	5
4	Stealing network credentials	4
5	Denial of service	8
Vulnerability after the implementation of proposed security Measures		27

Table 2. Types of possible Attacks on Virtual Reality after implementing the Security Measures

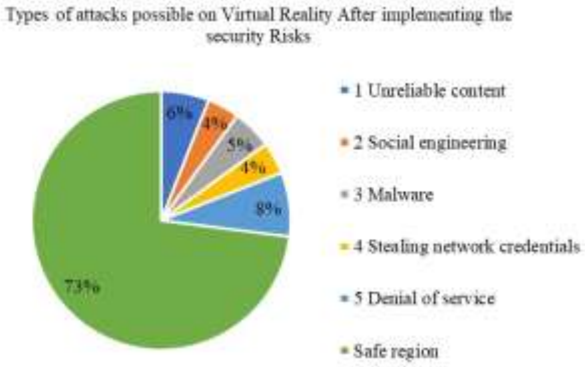


Fig.5.Risk before implementation of security Measures.

After implement the proposed security measures we have restricted most of the security threats from 100% to 27%.

V. CONCLUSION & FUTURE WORK

Even though several security measures are implemented using security protocols/firewalls which are unable to protect the vulnerabilities of VIRTUAL REALITY devices. Hackers/introduces are continuously making attempt to gain the unauthorized access of Virtual Reality devices using various attacks. As Virtual Reality devices usage has an effect on their usage. In order to protect the security and integrity of Virtual Reality devices several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Special study on virtual reality technology: virtual reality head-mounted display and interactive device" by sraSontisirkit. Asian institute of technology, school of engineering and technology, Thailand.

[2] Virtual reality society (2016) (information available at (http://www.vrs.org.uk/virtual-reality-environments/)

[3] M. Virvou, G. Katsionis, and K. Manos, "Combining software games with education: Evaluation of its educational effectiveness." Educational Technology.

[4] J. T. Bell and H. S. Fogler, "The application of virtual reality to chemical engineering education," VR, vol. 4,pp. 217–218, 2004

[5] June 2010 DOI:10.4018/978-1-60566-940-3.ch012 In book: Affective, Interactive and Cognitive Methods for E-Learning Design: Creating an Optimal Education Experience (pp.228-243) Edition: 1Chapter: 12Publisher: IGI GlobalEditors: Aimilia Tzanavari, Nicolas Tsapatsoulis

[6] William R. Sherman, Alan B. Craig, in Encyclopedia of Information Systems, 2003

[7] engineering, and mathematics education Author links open overlay panelRichard Lamb Show more Add to Mendeley Share Cite https://doi.org/10.1016/B978-0-12-818630 5.13075-1

[8] Introducing Virtual Reality Technologies to Design Education May 2018Seminar net 14(1) DOI:10.7577/seminar.2584 LicenseCC BY 4.0.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Cloud Computing : Fundamentals and Research Issues

N.Kavya,
23CSC28, Student, M.Sc.(Computer Science),
Dept. of Computer Scince,
P.B.Siddhartha College of Arts & Science
Vijayawada, A.P, India
monikakorivi91@gmail.com

P.Hafsa Begum,
23CSC31, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
Kavyasrii0143@gmail.com

K.Monika,
23CSC12, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B.Siddhartha College of Arts & Science,
Vijayawada, A.P, India.
Kavyasrii0143@gmail.com

Abstract- Cloud computing means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer's hard drive or local server. Cloud computing is also referred to as Internet-based computing, it is a technology where the resource is provided as a service through the Internet to the user. The data which is stored can be files, images, documents, or any other storable document. Cloud computing has taken its place all over the IT industries. It is an on-demand internet-based computing service that provides the maximum result with minimum resources cloud computing provides a service that does not require any physical close to the computer hardware. Cloud Computing is a product of grid, distributed, parallel, and ubiquitous computing. This paper introduces the concepts, history pros, and cons of cloud computing. Now coming to IoT, it can be any device equipment, or object which connects us with the cloud using the internet or with another device that is connected. It has sensors, processing ability, software, and many technologies which can be used to share and fetch data or information with other devices and servers over the internet. Nowadays big companies are using cloud services for storing their data because it is easy to manage their data easily without any additional costs.

I. INTRODUCTION

In cloud computing, Cloud Computing concept has emerged from the distributed software architecture. Cloud computed technology is aimed to provide hosted services over the internet. In recent years, cloud computing in Information Technology has given rise to various new user communities and markets [1]. Cloud computing is an on-demand service, through internet different servers physical and virtual. It is more hosted at remote data and managed by CSP.CSP provides some services subscription-based or fees or bills according to usage or user.By using the cloud we can get rid of purchasing, installing, and managing our infrastructure. This makes it easy for an organization to purchase and configure supporting hardware and make them use enterprise applications within minutes. we can scale capacity up and down according to response to spikes and dips in traffic. Over the years, with the development in Information Technology Industry, the demand for storing and computing resources growing bigger in the marketplace. [2]. Cloud Computing is a network-built handling invention where information is provided to customers on demand. Cloud Computing is a registering phase for dissemination of advantages and assets that involve structures, programming, applications, introduction and commerce. Distributed computing is a robotic supply of handling asset.

II. RELATED WORK

There are several security risks to consider when making the switch to cloud computing. Some of the top security risks of cloud computing include:

1. Limited visibility into network operations
2. Malware
3. Compliance
4. Data Leakage
5. Inadequate due diligence
6. Data breaches
7. Poor application programming interface (API)

Risks in Cloud Computing:

1. **Limited visibility into network operations.**
   When moving workloads and assets to the cloud, organizations forfeit a certain level of visibility into network operations. This is because the responsibility of managing some of the systems and policies shifts to the cloud service provider. Depending on the type of service model being used, the shift of responsibility may vary in scope. As a result, organizations must be able to monitor their network infrastructure without the use of network- based monitoring and logging.

2. **Malware**
   By moving large amounts of sensitive data to an internet-connected cloud environment, organizations are opening themselves up to additional cyber threats. Malware attacks are a common threat to cloud security, with studies showing that nearly 90% of organizations are more likely to experience data breaches as cloud usage increases. As cybercriminals continue to become increasingly savvy with their attack.
3. **Compliance**
   Data privacy is becoming a growing concern, and as a result, compliance regulations and industry standards such as GDPR, HIPAA, and PCI DSS are becoming more stringent. One of the keys to ensuring ongoing compliance is by overseeing who can access data and what exactly they can do with that access. Cloud systems typically allow for large-scale user access, so if the proper security measures (ie. access controls) aren’t in place, it can be difficult to monitor access across the network.
4. **Data Leakage**
   Data leakage is a growing concern for organizations, with over 60% citing it as their biggest cloud security concern. As previously mentioned, cloud computing requires organizations to give up some of their control to the CSP. This can mean that the security of some of your organization’s critical data may fall into the hands of someone outside of your IT department. If the cloud service provider experiences a breach or attack, your organization will not only lose its data and intellectual property but will also be held responsible for any resulting damages.
5. **Inadequate due diligence**
   The move to the cloud should not be taken lightly. Similar to a third-party vendor, when working with a cloud service provider, it’s important to conduct thorough due diligence to ensure that your organization has a complete understanding of the scope of work needed to successfully and efficiently move to the cloud. In many cases, organizations are unaware of how much work is involved in a transition and the cloud service provider’s security measures are often overlooked.
6. **Inadequate due diligence**
   The move to the cloud should not be taken lightly. Similar to a third-party vendor, when working with a cloud service provider, it’s important to conduct thorough due diligence to ensure that your organization has a complete understanding of the scope of work needed to successfully and efficiently move to the cloud. In many cases, organizations are unaware of how much work is involved in a transition and the cloud service provider’s security measures are often overlooked.
7. **Data breaches**
   One of the most impactful security risks the cloud faces is the potential for a data breach. These are a result of poor security measures that allow malicious actors to gain access to sensitive data across cloud servers. One breach could cost an organization millions of dollars, alongside a blow to an organization’s reputation and the potential for legal liability.
8. **Poor API**
   If the cloud has poor application program interfaces (API), then servers run the risk of having data unwillingly exposed. When it comes to API, malicious actors will employ several strategies such as brute force attacks and denial-of-service attacks in order to weaken the integrity of the system.

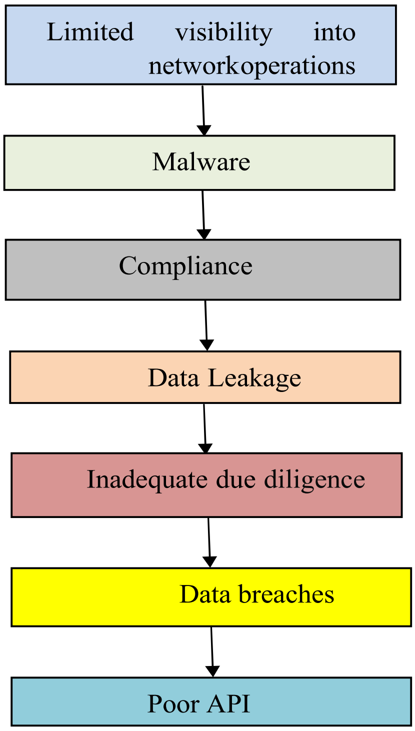


Fig.1. various risks in cloud computing

III. PROPOSED WORK

We propose the following security methods to prevent threats on Cloud Computing.

1. Security of Data:

This paper discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The paper will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have security loopholes in them.

2. Insufficiency of Resources and Expertise:
Hiring the right Cloud talent is another common challenge in cloud computing. There is a shortage of working security professionals with the necessary qualifications in the industry as the workloads are increasing, so are the number of tools launched in the market. The Best Way to Bypass Cloud Computing Skills Shortage Managed Cloud Services.

3. Complete Governance over IT Services:
IT always doesn't have full control over provisioning, infrastructure delivery, and operation in this cloud-based world. This has raised the complicacy of IT to offer important compliance, governance, data quality, and risk management.

4. Cloud Cost Management:
The Right Scale report revealed that for a few companies, handling cloud spending has passed security as the biggest cloud computing challenge. As per their anticipations, organizations are ruining nearly 30% of the money they invest in the cloud.

5. Dealing with Multi-Cloud Environments:
These days, maximum companies are not only working on a single cloud. As per the Flexera 2023 State of the Cloud Report, nearly 87% of the companies are following a multi-cloud strategy and 72% already have their hybrid cloud tactic that is combined with the public and private cloud. Furthermore, organizations are utilizing five distinct public and private clouds.

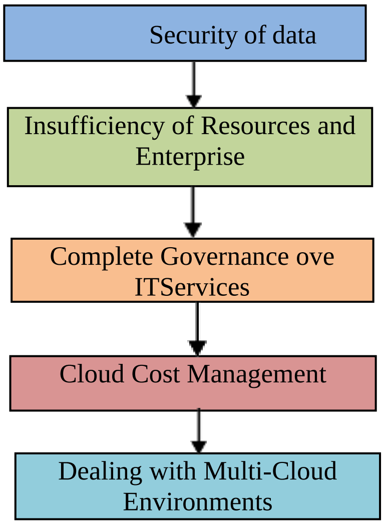

Security of data
Insufficiency of Resources and Enterprise
Complete Governance ove ITServices
Cloud Cost Management
Dealing with Multi-Cloud Environments

Fig.2.various measures in cloud computing

Algorithm:

1. Begin
2. Identify Potential Fog Computing Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End.

IV. RESULT & ANALYSIS

S. No.	Type of Attacks possible on cloud computing before implementing the security Measures	Percentage of Vulnerability
1	Limited visibility intonetwork operations	20
2	Malware	30
3	Compliance	14
4	Data leakage	15
5	Inadequate due diligence	10
6	Data Breaches	6
7	Poor API	5
Vulnerability before the implementation of proposedSecurity Measures		100

Table 1.Types of possible Attacks on cloud computing before implementing the Security Measures

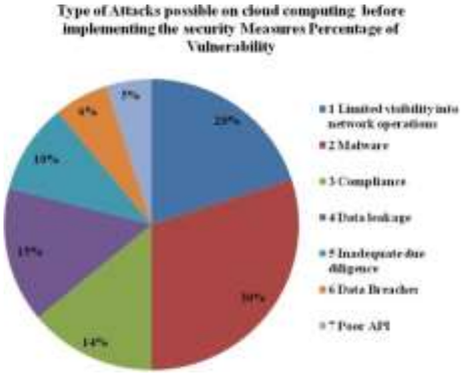


Fig.3. Risks before implementing ofSecurity Measures

S.No.	Type of Attacks possible on cloud computing after implementing the security Measures	Percentage of Vulnerability
1	Security of Data	10
2	Insufficiency of Resources and Expertise	5
3	Complete Governance over IT Services	6
4	Cloud Most Management	2
5	Dealing with Multi-Cloud Environments	7
Vulnerability before the implementation of proposed Security Measures		30

Table 2. Types of possible Attacks on cloud computing after implementing the Security Measures

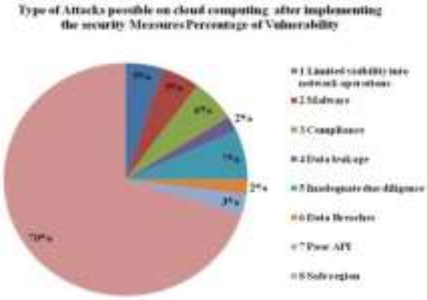


Fig. 4. Risks after implementation of Security Measures

After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION & FUTURE WORK

Even though several measures are implemented using security protocols /firewalls which are unable to protect the vulnerabilities of Fog Computing. Hackers/introduces are continuously making attempts to gain the unauthorized access of Fog Computing using various attacks. Fog Computing devices usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of Fog Computing several new security measures, protocols and firewalls needs to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] Bader alouffi ,"a systematic literature review On cloud computing security: threats and Mitigation strategies", 14 april 2021, DOI: 10.1109/ac cess.2021.3073203, electronic issn: 2169-3536.

[2] Neeraj singla , "a review paper on cloud computing", 23-24 december 2022, DOI: 10.1109/cisct55310.2022. 1004657, electronic isbn:978-1-6654-7416-0

[3] Gurmeher singh puri , "a review on cloud computing",10-11january2019, doi: 10.1109/confluence.2019.8776 907,electronic isbn:978-1-5386-5933-5 [4].

[4] Shyam patida , "a survey paper on cloud Computing", 07-08 january 2012 , DOI: 10.1109/acct.2012.15 , isbn:978-1-4673-0471-9 [5].

[5] San murugesan , "cloud computing", 2016, DOI: 10.1002/9781118821930.ch1,electronic isbn:9781118821961

[6] Sanchuan luo , "application of cloud computing in data information system management " ,14-16 october 2022, DOI: 10.1109/icinc58035.2022.00019,electronic isbn:979-8-3503-0969-0

[7] nader f. Mir , "cloud and edge computing", june 2020 ,doi: 10.1109/mcomstd.2020.9139038,electronic Issn: 2471-2833

[8] Sanae esseradi , "mobile cloud computing: current development and research challenges", 2730 may 2013, DOI: 10.1109/aiccsa.2013.6616482, Electronic isbn:978-1-4799-0792-2

[9] divyansha garg , "cyber attacks in cloud computing environment", 01-03 june 2023, DOI: 10.1109/icces57224.2023.10192833 , electronic isbn:979-8-3503-9663-8

[10] Jing liu , "ccra: cloud computing reference architecture",2429june2012,doi: 10.1109/scc.2012.110

[11] Savita devi , "study of architecture and issues in services of cloud computing", 17-18 december 2021,doi: 10.1109/icac3n53548.2021.9725679 , Electronic isbn:978-1-6654-3811-7

[12] Suyel namasudra , "cloud computing: fundamentals and research issues" ,05 october 2017,doi: 10.1109/icrtccm.2017.49 , electronic isbn:978-1-5090-4799-4.

Edge Computing Security Best Practices and Strategies

N.P.B.Siva Naga Mani,
23CSC29, Student, M.Sc. (Computer Science),
P.B. Siddartha College of Arts & Science,
Vijayawada, AP, India,
sivanagamaninunna@gmail.com

K.Hepsiba,
23CSC10, Student, M.Sc. (Computer Science,
P.B. Siddhartha College of Arts & Science,
Vijayawada, AP, India,
kolusuhepsiba@gmail.com

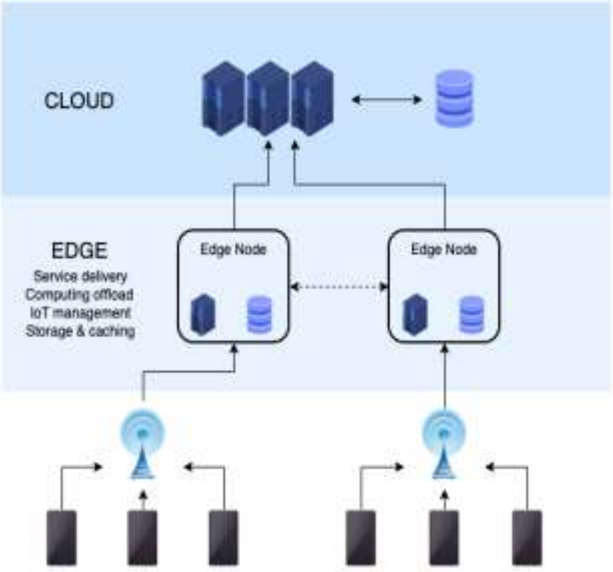
G.Prathyusha,
23CSC05, Student, M.Sc. (Computer Science),
P.B. Siddhartha College of Arts & Science,
Vijayawada, AP, India,
Prathyushagovada7@gmail.com

ABSTRACT: **The Edge Computing Is Facing Many Problems and Efforts Are Being Made to Overcome Those Challenges. Hybrid Mobile Edge Computing Is Introduced for The Mobile Devices to Overcome the Limited Battery Issues and Performance Constraints in The Devices. There Were Some Difficulties in The Integrated Development Environment of The Edge Computing, And to Overcome Those Problems, A Container-Based Method is Introduced Which Improves the Performance of The Coding Environment In EC, And Also It Facilitates In-Place Debugging. An EC Architecture Is Presented That Provides Local Data Processing, Management, And Quick Reaction for The Virtual Iot Devices. With EC's Support, A Hybrid Computing Framework Is Built and An Intelligent Resource Scheduling Strategy to Fulfil the Real-Time Requirements in Smart Manufacturing; Which Showed Satisfactory Results. A Multi-Source Transmission Protocol Is Presented to Counter Problems Such as The Low Video Streaming and High Bandwidth Usage.**

KEYWORDS: Evaluation, Streaming, Real, Resource, Task, Edge, Smart, Computing, Internet, Mobile, Remote, Container.

I. INTRODUCTION

One definition of edge computing is the use of any type of computer program that delivers low latency nearer to the requests. Karim arabi, in an IEEE DAC 2014 Keynote and subsequently in an invited talk at MIT's MTL Seminar in 2015, defined edge computing broadly as all computing outside the cloud happening at the edge of the network, and more specifically in applications where real-time processing of data is required. The term is often used as synonymous with fog computing. This especially is quite relevant for small deployments. However, when the deployment size is large, e.g., for Smart Cities, fog computing can be a distinct layer between the Edge and the Cloud. Hence in such deployments, Edge layer is a distinct layer too which has specific responsibilities. According to The State of the Edge report, edge computing concentrates on servers "in proximity to the last mile network". Alex Reznik, Chair of the ETSI MEC ISG standards committee, loosely defines the term by essentially suggesting that anything that's not a traditional data centre could be the 'edge' for somebody.



Edge nodes used for game streaming are known as game lets, which are usually one or two hops away from the client. Per Anand and Edwin say "the edge node is mostly one or two hops away from the mobile client to meet the response time constraints for real-time games' in the cloud gaming context." Edge computing may employ virtualization technology to make it easier to deploy and run a wide range of applications on edge servers. The world's data is expected to grow 61 percent to 175 zettabytes by 2025. According to research firm Gartner, around 10 percent of enterprise-generated data is created and processed outside a traditional centralized data centre or cloud. By 2025, the firm predicts that this figure will reach 75 percent.

II. RELATED WORK

In this section, we exemplify various Security Risks in Edge Computing:

RISKS IN EDGE COMPUTING:

1. **Data storage, backup and protection risks:**
   Data stored at the edge, as already noted, lacks the physical security protections usually found in data centres. In fact, it might be possible to steal an entire database simply by removing the disk from the edge computing resource, or by inserting a memory stick to copy information. Because edge computing facilities often have limited local storage options, it might also be difficult or even impossible to back up critical files, which means if an incident occurs, there might not be a backup copy to restore the database.
2. **Password and authentication risks:**
   Edge computing resources are rarely supported by local IT operations professionals who are security conscious. In many cases, maintaining the edge systems might be a part-time job assigned to several people, and this situation encourages lax password discipline, including accepting default passwords, using simple passwords easily remembered, posting notes with passwords for critical applications and failure to change passwords often. Edge systems might not employ strong authentication measures such as multi-factor or two-stage authentication, again, for the convenience of users and administrators.
3. **Perimeter defence risk:**
   Because edge computing expands the IT perimeter, it complicates perimeter defence overall. Edge systems themselves might have to authenticate their applications with partner applications in the data centre, and the credentials for this are often stored at the edge. That means a breach of edge security might expose access credentials to data centre assets, increasing the scope of the security breach considerably. Because security tools might be limited at the edge by architecture differences in hosting, dealing with perimeter threats can be more difficult.
4. **Cloud computing risk:**
   Cloud computing remains the hottest topic in IT, overall, so the risks associated with edge computing in combination with cloud computing are particularly important. What those risks are depends on the specific relationship between edge and cloud – something that's easy to lose track of, because different cloud software platforms and services treat edge elements in different ways. If the edge devices are simple controllers, as is often the case, it can be difficult to give them secure access to cloud resources and applications. That makes the evaluation of cloud-to-edge connection, access control and general security measures especially important.
5. **Edge and IOT security risks:**
   Edge applications relating to IOT pose special security risks because IOT devices are designed for low cost, low power usage and deployment to areas often not suitable for complex technology because of conditions in the environment where they're deployed, such as temperature and humidity, dust or vibration.

These risks include the following:

Use of specialized M2M protocols, which normally lack sophisticated security features such as encryption; Wireless interfaces such as Wi-Fi, which could be subject to hacking or hijacking because of easy access to the area where the Wi-Fi hubs are installed; and dependence on specialized IOT or industrial controllers as edge computing resources, when these specialized devices are difficult for users to upgrade with proper security software.

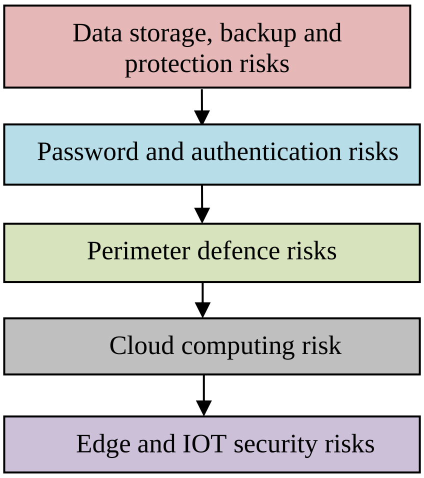

Data storage, backup and protection risks
Password and authentication risks
Perimeter defence risks
Cloud computing risk
Edge and IOT security risks

Fig.1. Risks in Edge Computing

III. PROPOSED WORK

MEASURES TO OVERCOME FROM TO SECURITY RISKS:

1. **Update and upgrade software:**
   Apply all software updates as soon as they are available. Ideally, you should automate this. Cyber criminals can engineer exploits almost as soon as a patch is released. Many vendors offer update services that help with automation; just be sure to use updates delivered through protected links and to test them prior to production release.

2. **Limit and control account access:**
   Threat actors gather account credentials, so it’s recommended that you start your program with a zero-trust framework. Under this model, account privileges are assigned sparingly only as users need them. Have documented procedures for securely resetting credentials or use a privileged access management tool to automate credential management. Also, update your on boarding and off boarding procedures to align with a zero-trust approach.

3. **Data Encryption:**
   Encrypt data both in transit and at rest to protect it from unauthorized access. Use secure communication protocols such as TLS (Transport Layer Security) for data transmission.

4. **Formalize a disaster recovery plan:**
   Your plan should start with business continuity and address data protection, data restoration, offsite backups, system reconstitution, configurations and logs. Remember, a DRP is not a static document; it should be continuously reviewed and updated. Building periodic reviews into your overall cyber security risk management plan will help identify any gaps,
5. **Privacy Protection:**
   In order to protect sensitive data, in edge computing, a privacy- preserving algorithm may be run between the cloud server and the edge server or the end device and the edge server. Location Privacy In edge computing, the location privacy mainly refers to the location privacy of the edge device users.

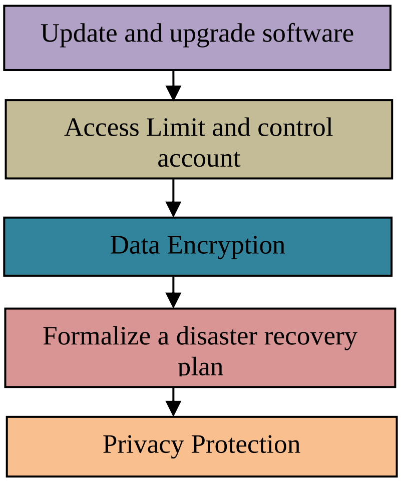

Update and upgrade software
Access Limit and control account
Data Encryption
Formalize a disaster recovery plan
Privacy Protection

Fig.2. Measures in Edge Computing

Algorithm:
1. Begin
2. Identify potential Edge Computing Security Threats.
3. Focus on the most probable Threats that could Harm Resources.
4. Determine Security Measures to protect Resources.
5. Put in place Measures to Effectively Protect Resources.
6. Asses the level of security to prevent Unauthorized Access.
7. End

IV. RESULT & ANALYSIS

S. NO	Typing of Attacks Possible on Edge Computing before implementing the security measures	Percentage of Vulnerability
1	Data storage, backup and protection risks	25
2	Password and authentication risks	27
3	Perimeter defence risk	22
4	Cloud computing risk	16
5	Edge and IOT security risk	10
Vulnerability before the implementation of proposed security measures		100

Table1. Types of possible Attacks on Edge computing before implementing the security measures

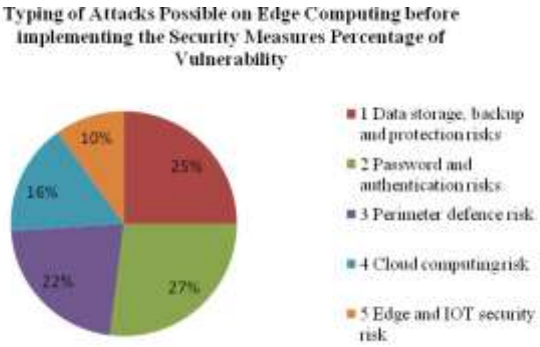


Fig.1. Risks before implementation security measures

S. NO	Typing of Attacks Possible on Edge Computing before implementing the security measures	Percentage of Vulnerability
1	Update and upgrade software	10
2	Limit and control account access	5
3	Data Encryption	6
4	Formalize a disaster recovery plan	5
5	Privacy Protection	4
Vulnerability before the implementation of proposed security measures		30

Table 2. Types of possible attacks on Edge computing after implementing the security measures

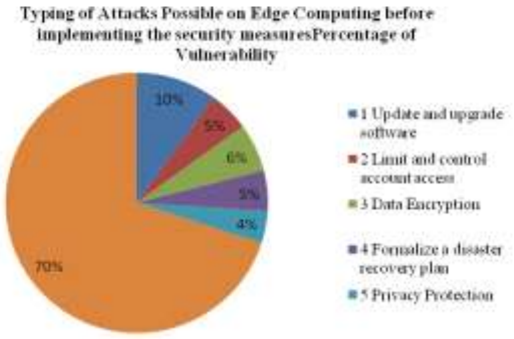
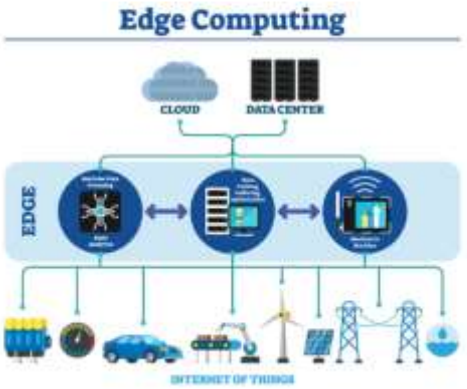


Fig.2.Risk before implementation of security measures of edge Computing

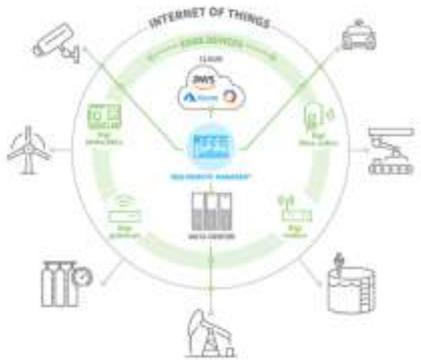
How Does Edge Computing Work?

Edge computing works by capturing and processing information as close to the source of the data or desired event as possible. It relies on sensors, computing devices and machinery to collect data and feed it to edge servers or the cloud. Depending on the desired task and outcome, this data might feed analytics and machine learning systems, deliver automation capabilities or offer visibility into the current state of a device, system or product.

Real-Life Use Cases for Edge Computing

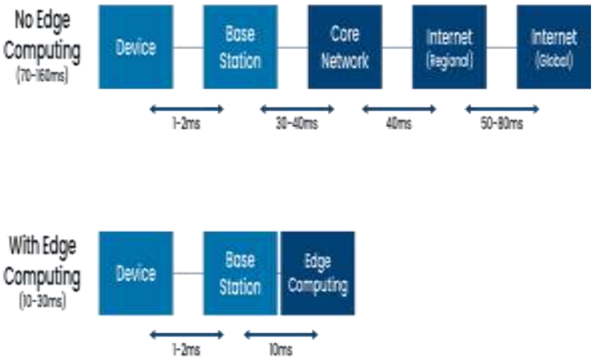


Depending on how many of the 30 billion Internets of Things (IoT) devices forecast for global deployment by 2020 rely on the cloud, managing the deluge of IoT-generated data makes proper processing seem near impossible. Traditional cloud computing has serious disadvantages, including data security threats, performance issues, and growing operational costs. Because most data saved in the cloud has little significance and is rarely used, it becomes a waste of resources and storage space.



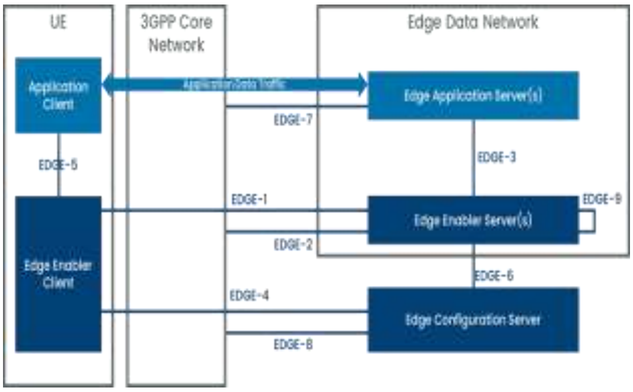
Why Edge Computing?

The most prominent benefit of edge computing is the reduced latency. Taking an illustrative example below (Figure 1) for a 5G network, one observes that it is possible to reduce the latency significantly (factor of 2 to 10 depending on assumptions) with edge computing.



Edge enabler layer

The edge enabler layer provides Application Programming Interfaces (APIs) for the application developers to leverage edge capabilities. With this layer, the application developers are able to locate, connect, and switch to the most suitable application server on the edge network, and to exploit the potential of the underlying 3GPP network in optimizing the service.



After implement the proposed security measures we have restricted most of the security threats from 100% to 30%.

V. CONCLUSION

IoT devices are gaining momentum from wearable's to vehicles to robots. As we are moving to a world with lots and lots of data, and data processing the need of a faster connection is becoming crucial. While a centralized data centre or cloud for data management, processing and storage has its limitations. Edge computing can provide an alternative solution for this. But since the technology is still in its immaturity, it is difficult to predict its success in future. Even though, there will be more opportunities for companies to test and set up this technology.

VI. REFERENCES

[1] "ETSI- ETSIBlog - What is Edge?" www.etsi.org.Retrieved 2019-02 19. https://www.etsi.org/newsroom/blogs/entry/what-is-edge
[2] https://www.stateoftheedge.com/
[3] "10 things you should know about Telco edge computing". www.linkedin.com
[4] https://www.cbinsights.com/research/what-is-edge computing/
[5] https://justmachinelearning.com/2019/01/03/what-is-edgecomputing/
[6] An Introduction to Edge Computing and A Real-Time Capable Server Architecture. Article available online https://www.researchgate.net/publication/326441179_An_Introduction_to_Edge_Computing_and_A_RealTime_Capable_Server_Architecture
[7] A Comparative Study of Fault Tolerance Techniques In Cloud Computing Secede Selma Madani1, Sharma Jamali International Journal Of Research In Computer Applications And Robotics Issn 2320-7345
[8] https://www.ge.com/digital/blog/what-edge-computing
[9] A Survey on the Edge Computing for the Internet of Things https://ieeexplore.ieee.org/document/8123913.
[10] Article: An Edge Computing Based Smart Healthcare Framework for Resource Management Soraia Ouida, Yahiya Kolb, Omayyad Allowably, Yasser Jararweh and Tar Baker: https://www.researchgate.net/publication/329479401_An_Edge_Computing_Based_Smart_Healthcare_Framework_for_Resoucrce_Management
[11] Edge Computing: Vision and Challenges; Wising Shi, JieCao, Quan Zhang, Youhunizi Li, Lanyon Xu. IEEE Internet of Things Journal Vol.3 No. 5 October 2016.

PARVATHANENI BRAHMAYYA(P.B.)
SIDDHARTHA COLLEGE OF ARTS & SCIENCE
VIJAYAWADA, ANDHRA PRADESH
Autonomous Since 1988 NAAC Accredited at 'A+' (Cycle III) ISO 9001:2015 Certified

Security Risks and Challenges of Blockchain

Dhanunjay Maddali,
23CSC34, Student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B. Siddhartha College of Arts& Science,
Vijayawada, A.P, India
maddalidhanunjay111@gmail.com

Bhargav Gujjala,
23CSC06, student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B. Siddhartha College of Arts& Science,
Vijayawada, A.P, India
bhargavgujjala@gmail.com

Ch.Lokesh,
23CSC19, student, M.Sc.(Computer Science),
Dept. of Computer Science,
P.B. Siddhartha College of Arts& Science,
Vijayawada, A.P, India
Chakkalokesh2002@gmail.com

ABSTRACT: In This Exploration of Blockchain's Impact on Finance, We Dissect the Landscape, Examining the Transformative Potential and Associated Challenges. Delving into Security Considerations, Regulatory Compliance, Interoperability, Scalability, And Privacy, This Article Provides Insights into Fortifying Financial Systems Against Risks. Discover Strategies to Harness the Benefits of Blockchain While Navigating the Evolving Regulatory Environment, Ensuring Security, And Maintaining the Delicate Balance Between Transparency and Data Protection. This Article Discusses Various Types of Attacks That Intruders or Hackers Can Carry Out to Gain Unauthorized Access Over Fog Computing Technologies. It Also Presents Measures to Minimize These Attacks on Resources of Blockchain Technologies In Finance. The Article Conducts A Thorough Examination of The Likelihood of Security Threats and Explores Various Ways to Minimize the Risks of Hacking, Providing Recommendations to Enhance Security.

I. INTRODUCTION

ENERGY is a natural resource that has been driving our economy for the past few decades. Increasingly, as our society becomes more digitalized and sophisticated, so does our reliance on energy. For example, according to the “BP Statistical Review of World Energy” [1], it was estimated that global primary energy demand grew by 2.9% in 2018, which is the fastest growth, since 2010. At the same time, carbon emissions Manuscript received February 16, 2020; revised May 21, 2020; accepted May 24, 2020. This work was supported in part by the National Natural Science Foundation of China under Grants 61972294 and 61932016 and in part by the Guangxi Key Laboratory of Trusted Software under Grant kx202001. The work of Kim-Kwang Raymond Choo was supported by the Cloud Technology Endowed Professorship and National Science Foundation CREST under Grant HRD-1736209. (Corresponding author:Debiao He.) Jiabin Bao is with the Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China. Debiao He is with the Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China, and also with the Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China. Min Luo is with the Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China. Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249 USA [1]. Distributed trading platform. from energy use grew by 2.0%, which is reportedly the fastest expansion for many years. The demand for natural gas has also reportedly increased by 5.3%, one of its strongest growth rates for over three decades. Coal demand (1.4%) also increased for the second consecutive year, following three years of decline. Growth in renewable energy (14.5%) decreased slightly but it is still the world’s fastest-growing energy source. Fossil fuels (nonrenewable energy) are limited, and it has been estimated that they will run out in the early 22nd century at the current rate of consumption [2]. This shortage and the known environmental issues associated with carbon emissions, have contributed to an increased focus in explore alternative sources of energy, most notable renewable energy sources such as solar and wind energy. For example, householder owners can install solar photovoltaic power generation system in their own houses for self-use, and the surplus electricity can be uploaded to the grid for financial rebates (i.e., consumers becoming procurers—see also Fig. 1). One challenge associated with such a trend is the management of the large, dynamic number of procurers. Conventional grid generally uses a centralized management system, which does not scale well or is not suitable for managing the large number of procurers. The cost of management and maintenance will also be prohibitively high in a conventional centralized management mode, in addition to the need to deal with challenges due to different (or lack of common) standards, and lack of mutual trust among participants. This necessitates the design of an efficient, safe, fair, and sustainable smart grid system. In addition, the increasing use of electric cars will compound the challenge of future smart grid system designs. Electric vehicles (EVs) are growing rapidly, with global sales of more than 5.1 million

EVs in 2018. It is estimated thatglobal sales of EVs 1937-9234 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. Content is final as presented, with the exception of pagination. 2 IEEE SYSTEMS JOURNAL Fig. 2. Applications of block chain. will reach 23 million and inventories will exceed 130 million by 2030 [3]. Existing challenges include inadequate supporting infrastructure (e.g., mobile and quick charging), as it is costly to uniformly deploy basic charging facilities. Thus, this also reinforces the importance of developing decentralized mobile charging. Hence, we also need to consider management, pricing, and privacy protection issues associated with the decentralized mobile charging infrastructure. The carbon emission trading system and green certificate trading system are market mechanisms used to promote global greenhouse gas emission reduction. Carbon trading enables trading institutions that cannot reduce their emissions to compensate by buying credits from others that meet their targets. Green certificates, on the other hand, provide green energy certificates to companies that use renewable energy sources to generate electricity, giving them subsidies to sell green energy. In the promotion of carbon emission trading system and green certificate trading system, users need to consider the safety, transparency and credit data registration of participants in the trading process. The preceding discussions emphasize the importance of decentralization, one trait commonly associated with block chain [4]. In recent years, the utility of block chain has explored in many applications, such as data management [5], [6], healthcare [7], [8], supply chain [9], Internet of Things (It) [10], [11], software-defined networking [12], cyber security [13], [14], etc. (see Fig. 2). Another popular application of block chain is in the energy area [15], [16], partly due to its underpinning characteristics such as anonymity, decentralization, transparency, and reliability. As mentioned above, as the energy sector becomes distributed, there are many issues that need to be addressed, such as distributed storage, control, management, trading, etc. These problems cannot be solved by traditional energy systems, while the features of block chain can provide solutions. The practical utility is also evidenced by the interest from major technology organizations, such as Siemens (investments in block chain development), and IBM (setting up a dedicated block chain lab to develop block chain applications for various areas, including a carbon tracking platform in China’s emissions-trading system and a project with the European power system operator, Tenet, to balance supply and demand for high-voltage grids).

II. RELATED WORK

Security risks and challenges of block chain:

1. Security Vulnerabilities:

Risk: Block chain's security is often lauded, but vulnerabilities exist, especially in decentralized applications (D-Apps) and smart contracts. Malicious actors may exploit weaknesses in the code, leading to significant financial losses.

2. Regulatory Uncertainty:

Risk: The regulatory landscape for block chain is dynamic and varies globally. Lack of clarity on compliance standards can pose legal challenges for businesses, leading to fines and operational disruptions.

3. Scalability Challenges:

Risk: As block chain networks grow, scalability becomes a pressing concern. Increased transaction volumes may result in slower processing times and higher fees, limiting the technology's efficiency.

4. Smart Contract Risks:

Risk: Smart contracts, while automating processes, are susceptible to coding errors, bugs, and vulnerabilities. Exploitation of these weaknesses can lead to financial losses and legal disputes.

5. Interoperability Challenges:

Risk: Lack of standardized protocols and interoperability between different block chain platforms can hinder seamless communication and asset transfer between networks.

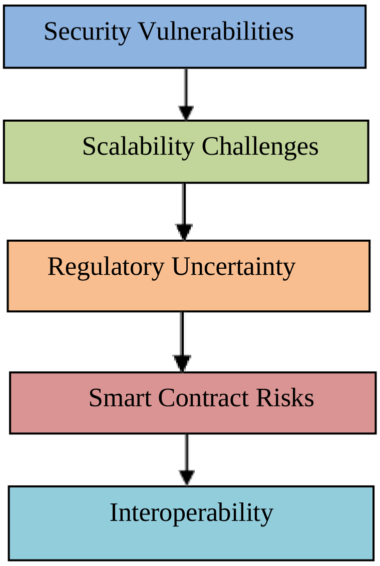


Fig.1. various security risks in block chain.

III. PROPOSED WORK

MEASURES OF BLOCK CHAIN:

1. Use Cryptography:

Measure: Utilize robust cryptographic algorithms to secure transactions and data on the block chain. Encryption techniques, such as public-key cryptography, play a crucial role in maintaining the integrity and confidentiality of information.

2. Maintain Consensus Mechanisms:

Measure: Choose an appropriate consensus mechanism based on the specific requirements of the block chain network. While proof-of-work is known for its security, it can be energy-intensive. Alternatives like proof-of-stake and delegated proof-of-stake offer energy efficiency and scalability. Tailor the consensus mechanism to balance security, decentralization, and efficiency.

3. Conduct Smart Contract Auditing:
Measure: Before deploying smart contracts on the block chain, conduct thorough audits to identify and rectify potential vulnerabilities and bugs. Collaborate with experienced smart contract auditors to ensure the reliability and security of the code.

4. Regular Network Upgrades are required:
Measure: Keep the block chain protocol up-to-date by implementing regular network upgrades. This ensures that the network can adapt to changing security requirements, incorporate new features, and address any identified vulnerabilities.
Measure: Maintain a decentralized network architecture to prevent single points of failure and enhance the security and resilience of the block chain. Avoid concentration of control in a few nodes or entities, promoting a distributed and democratic network.

5. Decentralization of resources is required:
Measure: Maintain a decentralized network architecture to prevent single points of failure and enhance the security and resilience of the block chain. Avoid concentration of control in a few nodes or entities, promoting.

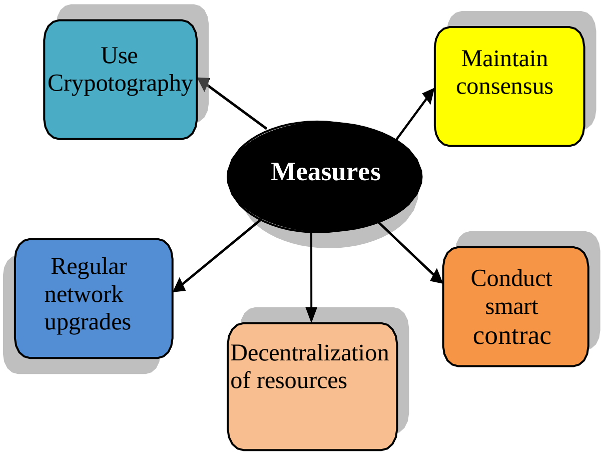


Fig.2. Various Measures of Block chain

Algorithm:
1. Begin
2. Identify Potential Block chain in threats.
3. Focus on the most probable Threats that could Harm resources.
4. Determine security measures to protect resources.
5. Put in place measures to effectively protect resources.
6. Assess the Level of Security to prevent Unauthorized Access.
7. End

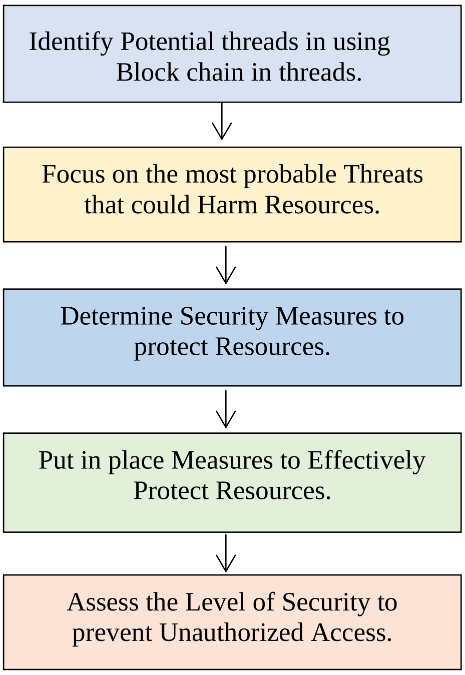

Identify Potential threads in using Block chain in threads.
Focus on the most probable Threats that could Harm Resources.
Determine Security Measures to protect Resources.
Put in place Measures to Effectively Protect Resources.
Assess the Level of Security to prevent Unauthorized Access.

Fig. 3. Procedure to safeguard the resources of securing threads.

IV. RESULT & ANALYSIS

S.No	Types of Attacks possible on Block Chain Technology before implementing the security Measures	Percentage of Vulnerability
1	Security Vulnerabilities	17
2	Regulatory Uncertainty	19
3	Scalability Challenges	22
4	Smart Contract Risks	16
5	Interoperability Challenges	26
Vulnerability before the implementation of proposed Security Measures		100

Table 1. Types of possible Attacks on Block Chain before implementing the Security Measures.

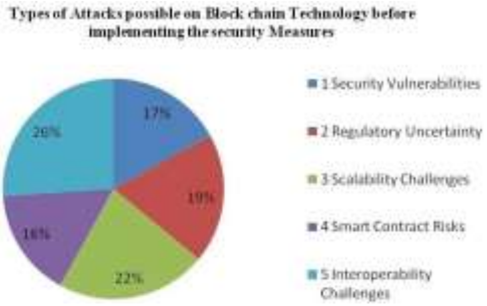


Fig. 4. Types of possible Attacks on Block Chain beforeImplementing the Security Measures

S.No	Types of Attacks possible on Block Chain Technology after implementing the security Measures	Percentage of Vulnerability
1	Security Vulnerabilities	5
2	Regulatory Uncertainty	8
3	Scalability Challenges	4
4	Smart Contract Risks	5
5	Interoperability Challenges	6
Vulnerability before the implementation of proposed Security Measures		28

Table 2. Types of possible Attacks on Block Chain After implementing the Security Measures.

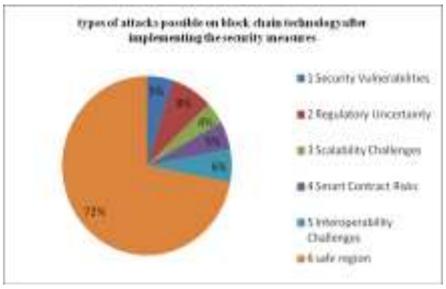


Fig.5. types of attacks possible on block chain technology after implementing the security measures

After implement the security measures we have restricted most of the security risks from 100% to 35%.

V. CONCLUSION & FUTURE WORK

Even though several security measures are implemented using several protocols/firewalls which are unable to protect the vulnerabilities of block chain. Hackers/introduces are continuously making attempt to gain the unauthorized access of block chain using various attacks as block chain usage has increased privacy and security challenges will have an effect on their usage. In order to protect the security and integrity of block chain several new security measures, protocols and firewalls need to developed and deployed effectively to challenge unauthorized access.

VI. REFERENCES

[1] OMAR ALI, Ashraf Jaradat, "BLOCK CHAIN" IN 21ST CENTURY PUBLISHED BY IEEE
DOI: 10.1109/ACCESS.2021.3050241

[2] BP, "Bp statistical review of world energy," 2019. [Online]. Available: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/ pdfs/energy-economics/statistical- review/bp-stats-review-2019-fullreport.pdf

[3] M. F. Hossain, "Solar energy integration into advanced building design for meeting energy demand and environment problem," Int. J. Energy Res., vol. 40, no. 9, pp. 1293–1300, 2016. [3] "Global EV outlook 2019 - International Energy Agency," 2019. [Online]. Available: https://www.iea.org/publications/reports/globalev outlook2019/

[4] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] E. Karafiloski and A. Mishev, "Block chain solutions for big data challenges: A literature review," in Proc. IEEE EUROCON 17th Int. Conf. Smart Technol., 2017, pp. 763– 768.

[6] W. Dai, C. Dai, K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A secure block chain-based data trading ecosystem," IEEE Trans. Inf. Forensics Secure., vol. 15, pp. 725–737, Jul. 2019.

[7] T. McGhin, K. R. Choo, C. Z. Liu, and D. He, "Block chain in healthcare applications: Research challenges and opportunities," J. Network Computer Appl., vol. 135, pp. 62–75, 2019.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using block chain for medical data access and permission management," in Proc. IEEE 2nd Int. Conf. Open Big Data, 2016, pp. 25–30.

[9] F. Tian, "An agri-food supply chain traceability system for china based on RFID & block chain technology," in Proc. IEEE 13th Int. Conf. Service Syst. Service Manage., 2016, pp. 1–6.

[10] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed block chain cloud architecture for It," IEEE Access, vol. 6, pp. 115–124, 2017.

[11] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Block chain applications for industry 4.0 and industrial IoT: A review," IEEE Access, vol. 7, pp. 17 6935–17 6951, 2019.

[12] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.

R. Choo, “P4- to-block chain: A secure block chain-enabled packet parser for software defined networking,” Computer. Secure., vol. 88, p. 101629,2020.