ARTICLE | OPEN ACCESS

Indian journal of
Engineering

To Cite:
Kanade A, Ranganthan CS, Babu AJ, Ramachandran G, Kusuma AK, Anand M, Reddy DVL. Analysis of wireless network security in internet of things and its applications. *Indian Journal of Engineering*, 2024, 21, e1ije1675
doi: https://doi.org/10.54905/disssi.v21i55.e1ije1675

Author Affiliation:
[1]Assistant Professor, Department of Computer Science and Applications, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India
[2]Associate Vice President, Mphasis Corporation, Chandler, Arizona, United States
[3]Professor, Department of computer Applications, School of Computing, Mohan Babu University, Tirupati, Andhra Pradesh, India
[4]Professor, Department of Electronics and Communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu, India
[5]Assistant Professor, Department of Physics, B V Raju Institute of Technology, Narsapur, Medak (Dist.), Telangana, India
[6]UG Student, Department of CS (IOT), Shiv Nadar University, Chennai, Tamil Nadu, India
[7]Assistant Professor, Humanities and social sciences department, JNTU College Of Engineering, Pulivendula-516390, Kadapa (D), Andhra Pradesh, India; Email: srichandrang@gmail.com

Peer-Review History
Received: 18 December 2023
Reviewed & Revised: 21/December/2023 to 16/February/2024
Accepted: 21 February 2024
Published: 27 February 2024

Peer-Review Model
External peer-review was done through double-blind method.

Indian Journal of Engineering
pISSN 2319–7757; eISSN 2319–7765

DISCOVERY
SCIENTIFIC SOCIETY

Analysis of wireless network security in internet of things and its applications

Anuradha Kanade[1], Chitra Sabapathy Ranganthan[2], Jyothi Babu A[3], Ramachandran G[4], Ashok Kumar Kusuma[5], Manav Anand[6], Lokeswar Reddy DV[7]

ABSTRACT

The study suggests a safety for networks risk analysis utilizing a network of a system to address security issues with the operation of Internet platforms, such as user privacy leaks. The survey system fully utilizes big data, cloud computing, and other high-tech tools to precisely identify potential network security issues and attempt to notify users and relevant departments of any current security issues. Based on this, the survey system is also created as a little program that uses very little memory and can continuously identify the security threats in the network for users. This paper also underlines that to reduce network security accidents, users must not only fully utilize the system for assessing security risks but also develop a strong sense of network security awareness. Channel estimate technology has received a great deal of attention and study as a result of the ongoing Long-term evolution (LTE), adoption and enhancements in global communication technologies in recent years. Channel estimation is crucial for lowering bit error rates and enhancing wireless communication system security. To gain complete channel information, we discuss the two-dimensional DCT (Discrete Cosine Transform) channel estimate approach in this study. The channel estimation method is then simulated and examined. The simulation results demonstrate that the two-dimensional DCT channel estimation method has a more accurate estimation performance and can successfully address the error flat bottom issue in the large delay channel based on DCT transformation. As a result, it can effectively enhance the communication and transmission security of the LTE system.

Keywords: Cloud computing, Networks, Security, Safety, Wireless

1. INTRODUCTION

All walks of life have started introducing Internet technology recently as a result of the continued development and application of Internet technology, which shows that it has been warmly welcomed by all walks of life. Even though

Internet technology has achieved outstanding progress in many areas, it is important to keep in mind that it also poses significant hazards and difficulties. The community is currently concerned about network security issues due to the frequency of occurrences relating to network security. Network security incidents have sudden features. The Internet platform's broad application spectrum and quick transmission speed also contribute to the widespread distribution and complexity of network security issues.

IoT (Internet of Things)

The term "Internet of Things" is officially used in the media sector and first debuted there. In addition, the Internet of Things is a significant byproduct of the third information technology revolution and a crucial tool for national scientific and technological advancement (Alaskri et al., 2023). In essence, the so-called Internet of Things technology is a sort of cutting-edge science and technology that depends on the Internet as a platform. It combines with numerous branches of science and technology, including cloud computing, location, etc. Realizing the connections between items and subsequent information exchange between objects is its primary goal. Software for Internet access of Things is currently used mostly to connect objects and Internet platforms, which can communicate any object's pertinent information to network devices and then provide the information for consumers, need to see. The Internet of Things technology has numerous uses according to Bao et al., (2020). Currently, it is mostly utilized for precise item identification, position determination, tracking, management, and supervision of various kinds of objects.

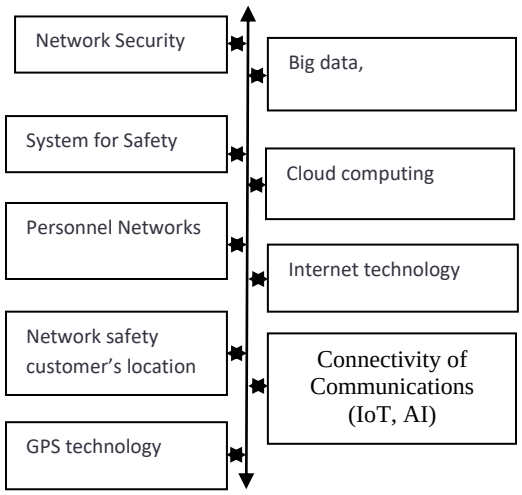

Figure 1 Block Diagram.

The Internet of Things' user end can exchange information with and communicate with any other object. The technology is to enable information flow between items and human-computer interaction (Dong et al., 2023), it encompasses a wide range of science and technology. Figure 1 depicts the genesis and progression of the items online and introduced the idea of the Internet of Things. At the time, "The Road to the Future" failed to capture the attention of the entire world. The "Internet of Things" concept was originally introduced in the Indian States by vehicles that rely mostly on item coding, RFID (Radio Frequency Identification) technology, and the Internet (Gu et al., 2023). The technologies that will fundamentally alter how people live their lives in the future.

In conclusion, research on Internet of Things technology focuses mostly on information sharing and human-computer interaction. Additionally, the science and technology encompassed by the Internet of Things have produced outstanding advancements in many important sectors and have significantly aided in advancing the cause of human scientific growth. Computer network can link up numerous unrelated machines to enable data transmission and exchange between them. In the era of computers, one of the primary functions of a computer is to facilitate data resource sharing and disseminate useful material to users (Hu and Heng, 2022). The five characteristics of modern network security are Confidentiality, Integrity, Usability, Safety and Controllability.

2. THE DESIGN AND OPERATION OF THE RISK INVESTIGATION SYSTEM FOR NETWORK

The Platform Architecture, first the tool uses SOA (Service-oriented architecture) and is built on the Android platform. Architecture design is integrated with cutting-edge mobile access technology, along with other high-tech elements, including wireless connection, database, and computer network security. The Internet of Things-based security risk investigation system may quickly identify security risk information in the network operation environment. Combined with the benefits of the Internet of Things for applications technology encompasses the fundamental layer, the data layer, the user layer, the application layer, and the application support layer. The system's fundamental layer serves as both the framework's bottom layer and the starting point for an analysis of network security issues. It is primarily made up of three components: the network communication system, the fundamental trusted terminal equipment, and the trusted service equipment (Khraisat and Alazab, 2021).

Layer 3 of Applications

The function of the application support layer is to give the application layer the essential fundamental support that is a crucial requirement for the application layer to play to its application advantages. The application layer would struggle to function well without the application support layer (Lian, 2021). Operating systems and frameworks, such as system integration frameworks, make up the majority of the system's application support layer. The primary responsibility of the system's application layer is to look into the covert threats to network security, keep an eye on the relevant network security status in real-time, and send users the results of this network monitoring (Liu et al., 2022). User layer: The purpose of the user layer, as its name suggests, is to offer services to users. Most users want to be able to quickly comprehend the most recent network security information. To prevent network security threats from materializing, users will be able to examine the network security information as soon as they log in.

Design Function

A portable law enforcement station - the system's mobile law enforcement component is based on the Android operating system and uses embedded development. Its job is to look into the site's security risks. Appropriate to the network environment's current security status. The foundational component of the mobile law enforcement end, which is mostly made up of many databases, is the network security information management module. It includes a variety of information, such as network security information generated by businesses and the personal network security information of citizens. It can aid law enforcement personnel in identifying potential network security vulnerabilities early on. The information operation element is a crucial component of mobile law enforcement. Its primary goal is to synchronize the system's data so that users can quickly identify the security risks in their network environments (Figure 2).

In addition, the module can quickly report network security problems to the network security law enforcement departments. The system’s mobile law enforcement end is not complete without the emergency rescue module. It integrates GIS (Geographic Information System) technologies to offer consumers GIS services. To correctly pinpoint the locations of network security concerns and relay those locations to authorities of network safety, and customers, it also uses GPS (Global Positioning System) technology (Li et al., 2022). The module can simultaneously create the optimum route for users and pinpoint the location of network security incidents. The personal information management the subdivision must keep the user's private data and offer a range of information management services, like timely updating the user's private data. In contrast to the personal information management module, the network information query module is a crucial component of the mobile law enforcement end.

While the network information query module focuses on retrieving information about current network security, which can help users better understand current network security, the personal information management module manages and stores users' personal information circumstance (Pei, 2021). End of service management, the system's service management portion uses SOA architecture, which is wholly focused on the mobile consumer segment. It can manage all types of mobile client data information and ease user and network security management personnel inquiry and storage, allowing users to monitor and assess the network security environment.

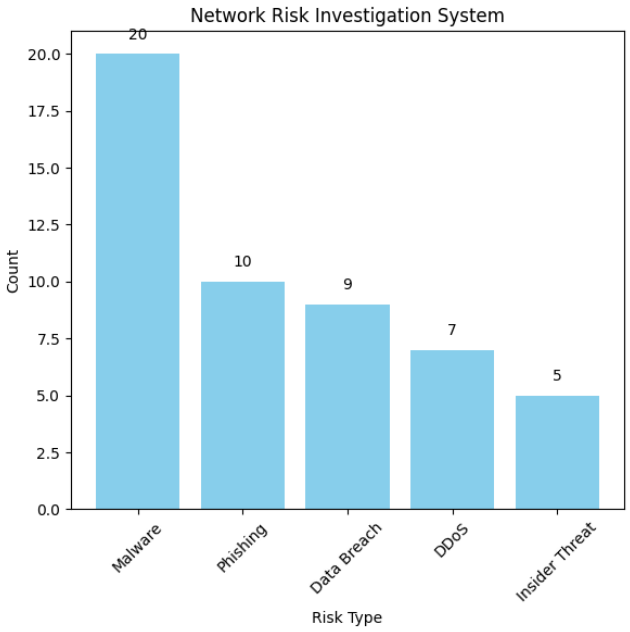

Figure 2 Network Security Design

Output personal network security

The network security information management module, the network security hidden danger management module, the network security accident handling module, the network security interactive communication module, and the network security emergency rescue command module are the main modules of the service management end of the system (Sudharsan and Ganesh, 2022).

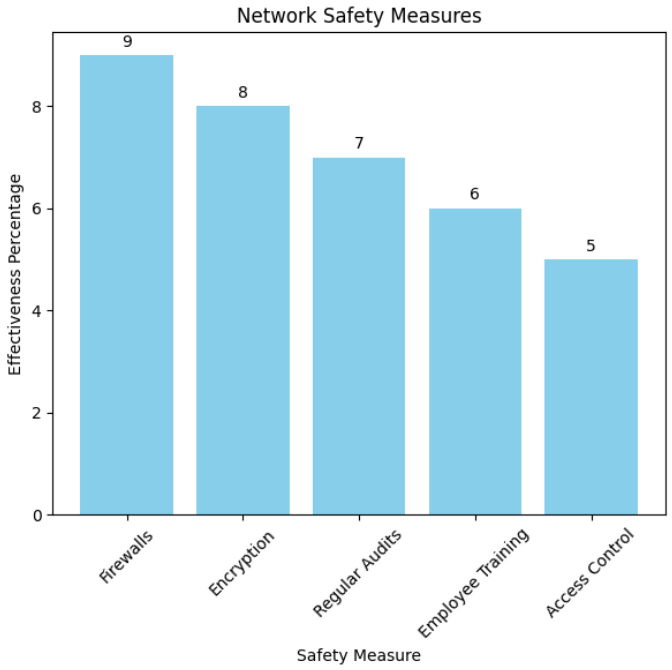

Figure 3 Safety security for personnel networks

Network security information management module, which can carry out daily upkeep of the network security environment and monitor all types of transmission information in the operation of the network in real-time. Additionally, it can offer customers other services like information modification and querying. The main module of the system and the service management end is the network security risk management module. Its primary duty is to promptly check the network operating environment's security (Sun and Wang, 2021). To decrease the chances of security breach accidents, the unit will instantly give feedback to the user when it discovers network security issues (Figure 3).

The service management end includes a module for handling network security incidents, which is very crucial. Its primary duty is to handle a variety of issues that arise following network security incidents (Figure 4). To give expertise for analyzing system safety risks and decreasing the component's chance of safety-related events can also save the network security incident information table filled out by the network security supervisors simultaneously. The goal of the network security interactive communication module is to increase Internet users' knowledge of network security from a variety of angles and expressions, hence lowering the likelihood of network security mishaps.

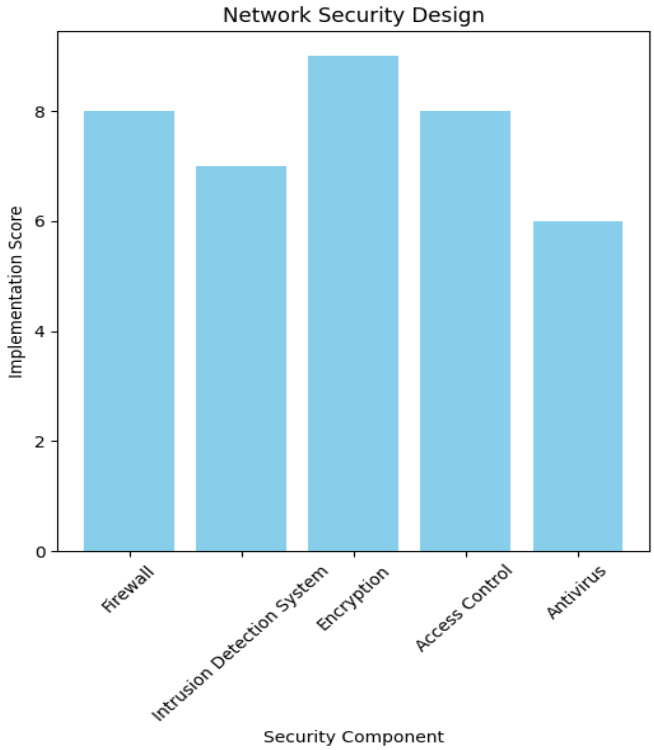

Figure 4 Output of personnel networks

The purpose of the network security emergency rescue command module is to gather, examine, and process all information about network security emergency rescue in real time to stop network security accidents in their tracks (Wu et al., 2020). Additionally, it can serve as a resource and source of experience for network security emergency rescue commands.

Hardware design

These extensions are serves for a variety of purposes, but they all aim to identify network security, concealed threats and lessen the likelihood of network security mishaps. Storage unit network security risks as well as create standards for investigating such risks in light of recent network security incidents (Figure 5); i.e. Positioning for Hidden Danger Information, Login Identity Authorization, Contrasting Hidden Risk, Database Information gathering about concealed danger, Data Information Processing review and correcting any hidden risks. Notification through SMS (Short Message Service) Information & Storage (Wang et al., 2022).

Figure 5 Network Security Risks Using the Internet of Things

LTE Systems with enhanced security

The latest generation Universal Mobile Telecommunication System (UMTS) standard, 3GPP (3rd Generation Partnership Project) Long Term Evolution, is continually being developed to fulfil the demands for high-speed device transmission in the mobile environment (Xiao et al., 2022).

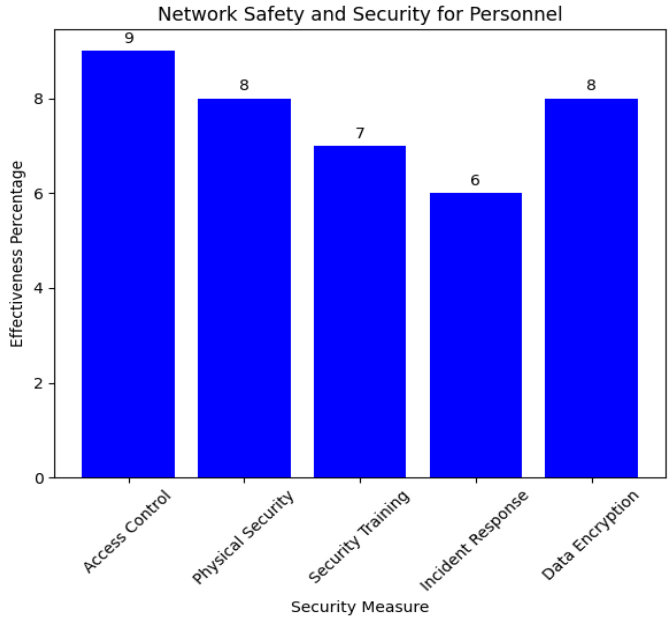

Figure 6 Output of personnel networks Mobile Phone and laptops

Time-based TDD (Time-Division Duplexing) mode and frequency-based FDD (Frequency Division Duplexing) mode are two separate duplex modes mixed in LTE baseband lines. Its peak rate can reach 100Mbps, and OFDMA (orthogonal frequency-division multiple access) technology is employed as its wireless access technology in the downlink system to enable the high flexibility and robustness demanded by the user in wireless resource allocation. The PAPR (Peak-to-Average Power Ratio) of the user terminal transmitter is reduced in the uplink system using SC-FDMA (Single-carrier-FDMA) technology, and the peak rate can approach 50Mbps. To enhance system performance, the LTE system additionally includes additional techniques such as MIMO (multiple-input multiple-output), a HARQ (Hybrid Autonomous Repetition Requests), and others (Xu et al., 2022). The anti-jamming capability and BER (Bit Error Rate) performance of the LTE system in a wireless environment are determined by the channel estimation performance, which serves as the system's key component (Figure 6). By computing the multipath channel's channel parameters and carrying out channel equalization, the channel estimation technique recovers the sent data and increases transmission reliability. OFDMA and SC-FDMA are the two main systems on which the channel estimate research for the LTE system is based.

The technique of channel estimation can be studied using one of two fundamental approaches the blind. The other is based on the pilot non-blind algorithm (Yan et al., 2021), while the former relies on the assessment of the transmitted data itself. The blind estimating procedure provides advantages in terms of data transmission rate and system delay since it does not require the insertion of the estimation pilot in the transmission frame structure. However, the drawbacks of a huge calculation quantity and limited flexibility result from the characteristics of blind estimating. In comparison to the blind estimation algorithm, the pilot-based non-blind algorithm has received significant attention in algorithm research and system implementation due to its relatively low system complexity, sensitive response to multi-path time-varying channels, flexibility in system application, and other characteristics. LTE systems also use such algorithms to improve the overall security of the transmission between the uplink and downlink (Figure 7).

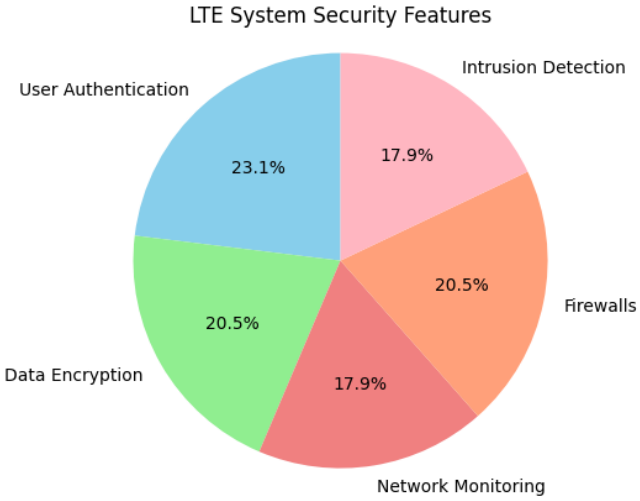

Figure 7 Output analysis system network safety customers location of network security

This is the channel estimate flow of an LTE system receiving connection (Zhang and Liu, 2021). After the subframe has been extracted, the invalid data (such as the cyclic prefix) must be eliminated. The frequency domain data is then calculated by FFR (Fast Fourier Transform) using the effective data in the subframe. The receiver extracts the pilot signal from the frequency-domain data per the pilot pattern, estimates the channel parameters of the pilot signal position, and then interpolates the channel parameters of all the time-frequency resource grid positions. To recover the original transmitter data, the channel characteristics and effective data of the associated resource grid site are determined.

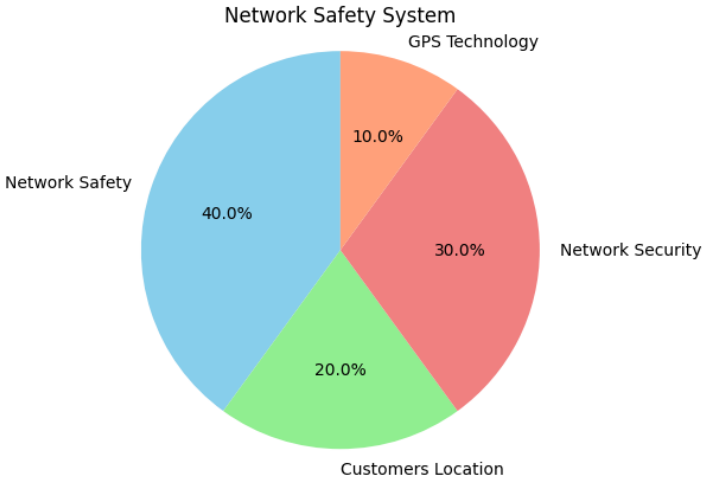

Figure 8 Applications of network security

When placed in the fixed location of the transmission signal, the pilot signal is a signal that is recognized by both the transmitter and the receiver. The pilot signal occurs as a reference signal (RS) in the LTE system. Resources are allocated to all signals in the LTE system using a resource grid structure, which allows for RS multiplexing in the LTE frame (Figure 8). In this study, the uplink employs the demodulated reference signal (DMRS) whereas the downlink uses the cell reference signal (CRS) designated by the LTE protocol for channel estimation.

3. RESULT AND DISCUSSION

The Wi-Fi play in Internet of Things systems to extract the most value from IoT environments and applications, Wi-Fi's integration and interoperability will allow IoT solutions to safely connect to billions of user-centric devices as well as to one another.

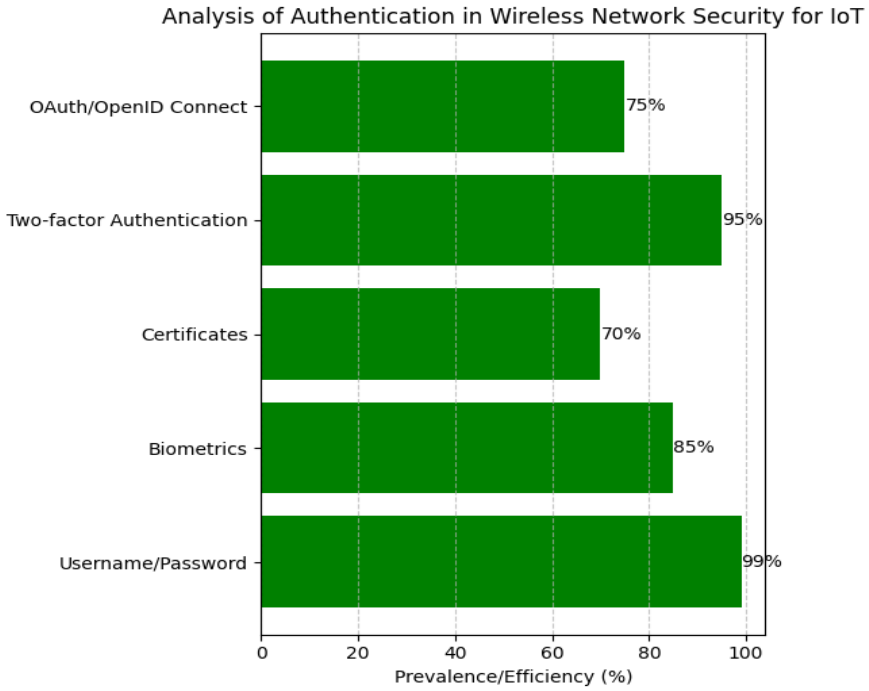

Figure 9 Analysis of Encryption Wireless Network Security in the Internet of Things and its Applications

The organization may become more profitable and agile as a result of new technological trends. However, the client was dealing with fresh issues related to Information technology (IT) security (Figure 9). Network Access Control (NAC) systems in each office to improve visibility and control over the network in order to address these security issues. The rapid proliferation of Internet of Things (IoT) devices, the shifting of workloads to the cloud, the growing use of virtualized services, and the surge in the Bring Your Own Device (BYOD) trend were all contributing to the rapid changes in the client's IT landscape. These modifications raised network vulnerability, decreased client control over network access, and decreased asset viability for end users and devices. The client was looking for a single pane of security and management infrastructure in light of these changes in order to lower operational costs brought on by manual labor and security mitigation.

The company is safe from new and emerging risks and stays ahead of the latest threats by keeping your network secure. To sum up, network security is essential to safeguarding your company's information. The integration of new technologies is propelling the Internet of Things' significant growth. Some of these more recent technological developments, like wearable, video, virtual and augmented reality, cognitive computing, and video, can scale and integrate with current systems. More developments are ahead for the future: - Faster: 5G, broadband wireless, Smaller: - micro and microscopic sensors Made Easier with 3D Printing, More Secure: - according to numerous reports, secure channels, digital certificates, and blockchain-enabled IoT devices will soon make up the majority of all globally networked devices.

Two studies were conducted (Figures 10 & 11) to assess the impact of incoming attacks on companies of various sizes. Small companies have fewer vulnerabilities in their network systems, making incoming attacks less likely. Vulnerabilities are difficult to discover and tackle. The Companies' defense systems are evaluated using many factors to determine their effectiveness. Minor changes to these parameters can cause system crashes or shutdowns. Improving security systems can greatly benefit firms of all sizes. Our simulation-based research uses a security-aware routing method to average the connection state of many topological trails and determine path connectivity.

Figure 10 Output of simulation system

Figure 11 Output of Live Network Transfer Security

The simulation system (Figure 10) helps system administrators understand how changing settings and security constraints impact network security. Figure 11 suggests that an agent-based system captures the dynamics of a company's network, including interactions between multiple agents such as attackers and defenders. A case study evaluates the proposed approach for assessing security threats in a company's network under various security rules (Zhou, 2021). This research proposes a novel security technique in chips based on industrial wireless network requirements. TV networks often use the same security measures as other networks, such as establishing a perimeter. However, there have been few studies on client-side device security.

4. CONCLUSION

In conclusion, based on the unique circumstances of this paper may track current network security occurrences in real-time and provide users and workplace security regulators with network security data information. The paper's numerical results lead to the following major conclusions. According to the author, the 4/4 l protection concealed trouble method of conducting a study using Internet of Things developments developed in this paper can improve inter-personal and inter-governmental cooperation, as well as the most effective way to stop computer security events at their origins is through the networking protection regulatory offices. They created a simulation-based study using the security-aware routing method to ensure secure wireless communication between two valid users over multiple topology trails.

Acknowledgement

This work is supported by Research on Security Wireless Monitoring and its Applications; We thank the participants who were all contributed

Author Contributions

Details of contribution of each authors regards manuscript work & production.

Ethical approval

This work is allowed for teaching and learning. Only proper citation of this work's content is permitted.

Informed consent
Not applicable.

Funding
This study has not received any external funding.

Conflict of Interest
The author declares that there are no conflicts of interests.

Data and materials availability
All data associated with this study are present in the paper.

REFERENCES

1. Alaskri A, Salem-Ahmed NA, Shaari H. Internet of Things (IoT): survey of most important security risks. 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, 2023; 295-299. doi: 10.1109/MI-STA57575.2023.10169291
2. Bao L, Wu S, Yu S, Huang J. Client-side Security Assessment and Security Protection Scheme for Smart TV Network. 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020; 573-578. doi: 10.1109/ICCC51575.2020.9345085
3. Dong W, Wang G, Yan Q, Liu Y. Design of Network Security Situation Awareness and Early Warning System Based on Big Data. 2023 International Conference on Networking, Informatics and Computing (ICNETIC), Palermo, Italy, 2023; 749-753. doi: 10.1109/ICNETIC59568.2023.00159
4. Gu J, Xia L, Wang H. Basic Network Construction and Network Security Design Analysis of Cloud Computing. 2023 2nd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2023; 1-6. doi: 10.1109/INOCON57975.2023.10101212
5. Hu B, Heng X. Research on 5G security protection system for Industry. 2022 International Conference on Informatics, Networking and Computing (ICINC), Nanjing, China, 2022; 142-146. doi: 10.1109/ICINC58035.2022.00036
6. Khraisat A, Alazab A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 2021; 4(1):1-27.
7. Li B, Zhai F, Fu Y, Xu B. Analysis of Network Security Protection of Smart Energy Meter. 2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2022; 718-722. doi: 10.1109/AEECA55500.2022.9918968
8. Lian J. Application of Computer Network Security Technology in Electronic Commerce. 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shanghai, China, 2021; 691-694. doi: 10.1109/AINIT54228.2021.00140
9. Liu Y, Xu L, Lin L. Remolding and Thinking of Network Security System in Intelligent Hospital. 2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC), Hangzhou, China, 2022; 80-83. doi: 10.1109/ICNISC57059.2022.00026
10. Pei S. Analysis of Scientific Research Cooperation Network in Cyberspace Security. 2021 IEEE 9th International Conference on Information, Communication and Networks (ICICN), Xi'an, China, 2021; 371-376. doi: 10.1109/ICICN52636.2021.9673815
11. Sudharsan R, Ganesh EN. A swish RNN based customer churn prediction for the telecom industry with a novel feature selection strategy. Conn Sci 2022; 34(1):1855-76. doi: 10.1080/09540091.2022.2083584
12. Sun D, Wang B. Research on the Design of the Implementation Plan of Network Security Level Protection of Information Security. 2021 7th International Symposium on Mechatronics and Industrial Informatics (ISMII), Zhuhai, China, 2021; 227-231. doi: 10.1109/ISMII52409.2021.00055
13. Wang L, Xie S, Cao C, Li C. Research on Security Service Model of Software Defined Network. 2022 6th International Symposium on Computer Science and Intelligent Control (ISCSIC), Beijing, China, 2022; 347-351. doi: 10.1109/ISCSIC57216.2022.00078
14. Wu X, Fu W, Mu D, Mao D, Zhang H, Zheng W. Improving the Security of Wireless Network Through Cross-project

Security Issue Prediction. 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 2020; 1179-1184. doi: 10.1109/ICCC49849.2020.9238816

15. Xiao W, Zhang X, Wang D. Cross-Security Domain Dynamic Orchestration Algorithm of Network Security Functions. 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), Guilin, China, 2022; 413-419. doi: 10.1109/DSC55868.2022.00063
16. Xu G, Zhou J, He Y. Network Malicious Traffic Detection Model Based on Combined Neural Network. 2022 6th Asian Conference on Artificial Intelligence Technology (ACAIT), Changzhou, China, 2022; 1-6. doi: 10.1109/ACAIT56212.2022.10137895
17. Yan W, Shu Q, Gao P. Security risk prevention and control deployment for 5G private industrial networks. In China Communications 2021; 18(9):167-174. doi: 10.23919/JCC.2021.09.013
18. Zhang Y, Liu C. An Immune Algorithm for Network Data Security Detection. 2021 17th International Conference on Computational Intelligence and Security (CIS), Chengdu, China, 2021; 247-251. doi: 10.1109/CIS54983.2021.00059
19. Zhou J. Construction of Computer Network Security Defense System Based On Big Data. 2021 International Conference on Big Data Analysis and Computer Science (BDACS), Kunming, China, 2021; 5-8. doi: 10.1109/BDACS53596.2021.00009