EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Research and Design of Encryption Standards Based on IoT Network Layer Information Security of Data

Jia Wang[1,*]

[1]Information and Electronics Department Neijiang Vocational & Technical College, Neijiang 641100, Sichuan, China

Abstract

INTRODUCTION: With the rapid development of the economy, more and more devices and sensors are connected to the Internet, and a large amount of data is transmitted in the network. However, this large-scale data transmission involves the problem of information security, especially in the transport layer. Therefore, there is an urgent need to study and design an information security data enhancement security strategy for the transport layer of ubiquitous networks (i.e., IoT).
OBJECTIVES: This thesis aims to research and create a data enhancement security strategy for the transport layer of the Ubiquitous Web to ensure the confidentiality and integrity of data transmitted in the Ubiquitous Web. Specific objectives include evaluating the advantages and disadvantages of current ubiquitous network transport layer lifting security techniques, proposing a new lifting security strategy applicable to the transport layer of ubiquitous networks, and verifying the feasibility and security of the proposed standard.
METHODS: First, a detailed study and evaluation of the current Ubiquitous Network Transport Layer Elevated Security Techniques is conducted, including analyzing and comparing the existing elevated security algorithms and protocols. Then, based on the obtained research results, a new lifting security strategy applicable to the transport layer of ubiquitous networks is proposed. The design process takes into account the characteristics and requirements of ubiquitous networks, such as resource constraints, dynamics of network topology, and cooperative communication of multiple devices. Subsequently, the feasibility and security of the proposed standard are verified through simulations and experiments. In the experiments, real ubiquitous network devices and network environments are used to evaluate the performance and attack resistance of the enhanced security algorithms.
RESULTS: Through the research and analysis of ubiquitous network transport layer lifting security techniques, some limitations of the existing lifting security algorithms are identified, such as high resource consumption, insufficient security, and limited ability to adapt to the characteristics of ubiquitous networks. Therefore, this thesis proposes a new lifting security strategy applicable to the transport layer of ubiquitous networks. The experimental results show that the standard can guarantee data confidentiality and integrity while possessing high efficiency and attack resistance. In addition, the proposed standard meets the needs of resource-constrained devices in ubiquitous networks and can operate properly under multiple network topologies and cooperative device communications.
CONCLUSION: This thesis proposes a new elevated security strategy applicable to ubiquitous networks through the study and design of transport layer elevated security techniques for ubiquitous networks. This standard can effectively protect the confidentiality and integrity of data transmitted in ubiquitous networks with high efficiency and attack resistance. The proposed standard is expected to provide a feasible solution for the information security of ubiquitous networks and a more reliable guarantee for developing and applying ubiquitous networks. Future work can further improve and optimize this enhanced security strategy and validate and apply it in a wider range of ubiquitous network environments.

Keywords: Internet of things, transport layer, information security, data enhancement security

Received on 12 February 2024, accepted on 26 April 2024, published on 2 May 2024

Copyright © 2024 Wang, licensed to EAI. This is an open-access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetsis.5826

*Corresponding Author. Email: dawang8084@163.com

1. Introduction

With the rapid development and wide application of sensor network technology, the author are in a highly interconnected digital era. Numerous devices and sensors interact and communicate via the Internet, generating large amounts of data every moment. However, it is this massive data transmission that also poses a major challenge to information confidentiality(Azrour et al., 2021). In sensor networks, transport layer data enhancement security is considered to be one of the most important means to protect the transmitted information. When data are transmitted over the Internet, they are exposed to the risk of unauthorized access and tampering. This risk can lead to leakage of sensitive information, theft of confidential data, and compromise of system integrity(Alavikia & Shabro, 2022). Therefore, transport layer data enhancement security in sensor networks becomes critical. Transport layer data elevated security refers to the elevated security of transmitted data at the transport layer of a sensor network to ensure the confidentiality and integrity of the data. Through the use of elevated security algorithms, the data is converted into ciphertext, which can be decrypted and restored to the original data only by the legitimate receiver who possesses the key(Sharma & Arya, 2023). This effectively prevents the risk of unauthorized third parties accessing sensitive information and tampering with data. It is of great significance and value to study the data enhancement security strategy based on the confidentiality of information in the transmission layer of sensor networks(Honar Pajooh et al., 2021). First, it can help protect the data transmitted in the sensor network from unauthorized access and tampering. This is crucial for protecting personal privacy, business secrets, and national security. Second, effective data enhancement security strategies can improve the security and trustworthiness of sensor network systems and enhance users' trust in sensor network technologies. In addition, the study can provide a basis for formulating relevant security policies and technical standards and promote the further development of sensor network technology. Therefore, the security challenges in sensor networks can be effectively addressed by conducting research in the sensor network transmission layer and designing data enhancement security strategies applicable to the sensor network environment(Li et al., 2021). This will provide strong support for building a more secure and stable sensor network environment. Future research should not only focus on the security of the boosted security algorithm but also consider resource consumption, performance optimization, and synergy with other sensor network components. The ultimate goal is to provide an efficient, reliable, and adaptable data enhancement security strategy to promote the healthy development of sensor network technology.

With the wide application of sensor network technology in various fields, data transmission in sensor network networks faces increasingly severe security challenges. Traditional transport layer data enhancement security algorithms often find it difficult to meet specific security requirements in sensor network environments and suffer from insufficient security, high resource consumption, and poor performance(Sharma & Arya, 2023). The characteristics of sensor networks determine their unique needs for data enhancement security. First, the large number of devices in sensor networks requires data-enhanced security algorithms to efficiently handle large-scale data transfers. Second, devices in sensor networks usually have limited computational and storage resources; thus, the boosted security algorithms need to be able to operate in resource-constrained environments. In addition, devices in sensor networks may be distributed in different network environments, and the boosted security algorithms need cross-network applicability and interoperability(Peng et al., 2021). Therefore, in-depth research is necessary to design new data-boosting security policies applicable to the transport layer of sensor networks. Such a standard should be able to fully consider the characteristics of the sensor network environment and meet the security, efficiency, and scalability needs of data transmission.

The security and efficiency of data transmission can be improved by overcoming the limitations existing in traditional lifting security algorithms through in-depth study and design of lifting security strategies for information confidential data based on the transmission layer of sensor networks. This research aims to develop new lifting security algorithms adapted to the sensor network environment to meet the specific security requirements in the sensor network domain. First, the new boosted security strategy will effectively protect sensor network data from unauthorized access and tampering. It will employ more robust elevated security algorithms and protocols to prevent data eavesdropping, interception, and tampering(Wang et al., 2021). This will ensure confidentiality and integrity during data transmission, thus protecting sensor network devices' and users' privacy and sensitive information. Secondly, the risk of information leakage can be reduced by adopting an information confidentiality data enhancement security strategy based on the transmission layer of the sensor network. The large number and wide distribution of devices in a sensor network increases the risk of data attack or accidental leakage(Honar Pajooh et al., 2021). The new elevated security policy will employ advanced authentication and access control mechanisms to ensure that only authorized devices and users can access and manipulate the data(Rekha et al., 2023). This will greatly reduce the possibility of information leakage and protect the security of the sensor network system. In addition, by establishing a secure and reliable sensor network environment, sensor network application scenarios such as smart homes, intelligent transportation, and industrial control systems will be provided with higher information confidentiality assurance(Zaman et al., 2021). Devices and systems in these application scenarios will benefit from new and enhanced security strategies to ensure their data is fully protected during transmission and processing(Ahmad et al.,

2021). For example, in the smart home, the adoption of enhanced security policies for information confidentiality data at the sensor network transport layer can protect the privacy and security of family members from unauthorized access and control.

Similarly, in smart transportation and industrial control systems, such a standard can ensure secure communication of vehicles and industrial equipment against unauthorized operation and interference, thus maintaining the normal operation of the whole system(Mousavi et al., 2021). In conclusion, the study and design of information confidential data boosting security strategies based on the transmission layer of sensor networks is crucial to address the limitations of existing boosting security algorithms(Sadhu et al., 2022). It will improve the security and efficiency of data transmission, protect the data in sensor networks from unauthorized access and tampering, and establish a safe and reliable sensor network environment. Meanwhile, this research result will also provide higher information confidentiality assurance for various sensor network application scenarios and promote the sustainable development of sensor network technology.

2. Background of the study

With the rapid development and wide application of sensor network technology, many connected devices and sensor-generated data continue to emerge, which prompts the need and importance of information confidentiality assurance in the transmission layer of sensor networks. Information confidentiality is particularly important in sensor networks because the transmitted data may contain sensitive information such as personal privacy and trade secrets. To ensure the security and efficiency of information transmission in the transmission layer of sensor networks, it becomes crucial to study and design data enhancement security strategies based on the transmission layer of sensor networks.

This research aims to conduct an in-depth study on the information confidentiality assurance needs of the transmission layer of sensor networks and the limitations of the current boosting security algorithms to design and innovatively propose a data-boosting security strategy adapted to the sensor network environment(Malhotra et al., 2021). With the rapid development of sensor networks, the transmission layer of sensor networks faces more and more information confidentiality challenges, such as data leakage, unauthorized access, and data tampering. The traditional boosted security algorithms have shown their limitations in facing the unique security requirements of sensor networks and cannot fully meet security assurance requirements(Abiodun et al., 2021). Through this research, the author are committed to improving the security and efficiency of data transmission in sensor networks. First, an in-depth understanding of the information confidentiality assurance needs of the transmission layer of sensor networks, including data confidentiality, integrity, and availability, will be presented. Understanding these requirements can help to understand the shortcomings of the current boosted security algorithms and explore innovative solutions. Second, to address the limitations of current boosted security algorithms in the sensor network environment, efforts will be made to propose a data-boosted security strategy adapted to the sensor network environment. Such a standard should be able to adapt to large-scale devices for boosted security communication data transmission with high real-time requirements, as well as low power consumption and high performance. Existing boosted security algorithms will be borrowed and innovatively designed to meet sensor networks' special needs to provide a stronger and more secure data protection mechanism(Bhuiyan et al., 2021). Through the research results, it is hoped that the data in the sensor network can be protected from the risk of unauthorized access and tampering. This will help to build a safe and secure sensor network environment, enabling individual user privacy to be protected, trade secrets to be kept confidential, and nationally important information to be secured. In addition, the research will also provide a higher level of information confidentiality assurance for various sensor network application scenarios, such as smart homes, intelligent transportation, and industrial control systems. In conclusion, the results of this research will provide an important theoretical foundation and practical solutions for improving the information confidentiality assurance capability of the transmission layer of sensor networks. The goal is to establish a secure and reliable sensor network environment to ensure the security and efficiency of data transmission, provide a better user experience, and promote the sustainable development of sensor network technology.

With the rapid development of sensor networks, traditional lifting security algorithms face many limitations and challenges. These traditional boosted security methods do not consider the special needs of sensor networks at the beginning of their design and thus cannot fully meet the specific security needs of sensor networks(Sarker et al., 2023). In particular, the limitations of traditional security enhancement algorithms become more obvious in sensor networks where there are large-scale devices for security enhancement communication and data transmission with high real-time requirements. In sensor networks, many devices need to communicate with boosted security, such as sensors and actuators in smart homes and sensors and actuators in industrial control systems(Ferrag et al., 2021). Conventional boosted security methods usually cannot effectively cope with the communication needs of such large-scale devices, leading to a decrease in the efficiency of data transmission. In addition, many application scenarios in sensor networks have high requirements for real-time data transmission. At the same time, the process of boosting security and decryption of traditional boosted security algorithms is usually time-consuming, making it difficult to meet the demands of real-time data transmission(Omolara et al., 2022). Therefore, it is of great significance to study and design a data-boosting security policy adapted to information confidentiality in the

transmission layer of sensor networks. Such a data enhancement security strategy should be able to fully consider the special needs of sensor networks and provide an efficient and secure enhancement security mechanism. When designing such a standard, it is necessary to provide scalable and high-efficiency solutions, considering the need for elevated security communication for large-scale devices(Karim, 2022). It also needs to address the security and efficiency of real-time data transmission to ensure that data can be transmitted promptly and securely. The security and efficiency of data transmission in sensor networks can be enhanced by researching and designing data enhancement security strategies adapted to the special needs of the transmission layer of sensor networks. This will help protect data in sensor networks from the risk of unauthorized access and tampering and establish a secure and reliable sensor network environment. In addition, such a standard will also promote the sustainable development of sensor network technology and the widespread use of sensor network applications.

In conclusion, with the rapid development of sensor networks, it is of great significance to study and design data-lifting security strategies adapted to information confidentiality in the transmission layer of sensor networks(Nyangaresi et al., 2022). By solving the limitations and challenges of traditional lifting security algorithms in sensor networks, the security and efficiency of data transmission can be improved, and the secure development of sensor networks can be promoted. This will create a safe and reliable sensor network environment for people and promote further application and innovation of sensor network technology. There are many security challenges in the current sensor network transmission layer, such as the risk of data leakage, unauthorized access, and data tampering. Traditional boosting security algorithms cannot fully meet the security needs of sensor networks, so innovatively designed data-boosting security strategies for sensor network environments are needed. The significance of this research is to improve the security and efficiency of data transmission in sensor networks and to protect the privacy and integrity of data(Abdullahi et al., 2022). This will play an important role in protecting individual user privacy, business secrets, and nationally important information and provide higher information confidentiality assurance for sensor network application scenarios, such as smart homes, intelligent transportation, and industrial control systems. This research will provide an important theoretical foundation and practical solutions for building a secure and reliable sensor network environment.

3. Research methodology

3.1 Problem analysis and data collection

The primary task of this research is to identify the key issues and challenges in the research and design of data enhancement security strategies based on information confidentiality in the Smart IoT transport layer. Specifically, the following questions are focused on the following: What are the potential security threats and attack methods in data transmission in the Smart IoT transport layer? What are the limitations and shortcomings of traditional data enhancement security policies when applying a smart IoT transport layer? What are the key functions and features need to be supported by the data enhancement security policy for the IOT transport layer? How can data enhancement security policies be researched and designed to adapt to the smart IoT transport layer to improve the security and reliability of data transmission?

This study aims to conduct in-depth research and overview of existing security strategies for information confidentiality and data enhancement in the transmission layer of Smart IoT to explore the current research progress and problems. Cases of data transmission security issues in real-world applications of the Smart IoT Transport Layer will be collected and analyzed to understand the needs and challenges faced in real-world applications. To comprehensively understand the security of the Smart IoT Transport Layer, interviews will be conducted with security experts in the Smart IoT Transport Layer, experts in elevated security technologies, and academic experts in related fields. The latest insights on the research and design of data enhancement security strategies will be obtained through the perspectives and recommendations of these experts.

Next, problem analysis and definition of requirements will be performed based on the collection and analysis of data. The key issues and requirements of the study will be defined through an in-depth analysis of the smart IoT transport layer security threats, the limitations of traditional enhancement security policies, and the requirements of the smart IoT transport layer. This will provide important guidance for subsequent research and design. This study is expected to provide an in-depth understanding of the current state of the art of information confidentiality and data enhancement security strategies for the Smart IoT transport layer and identify the current research's key issues and needs. This will provide important references and guidance for further improving and enhancing the security of the Smart IoT transport layer. The logic of the data enhancement security technology is shown in Figure 1.

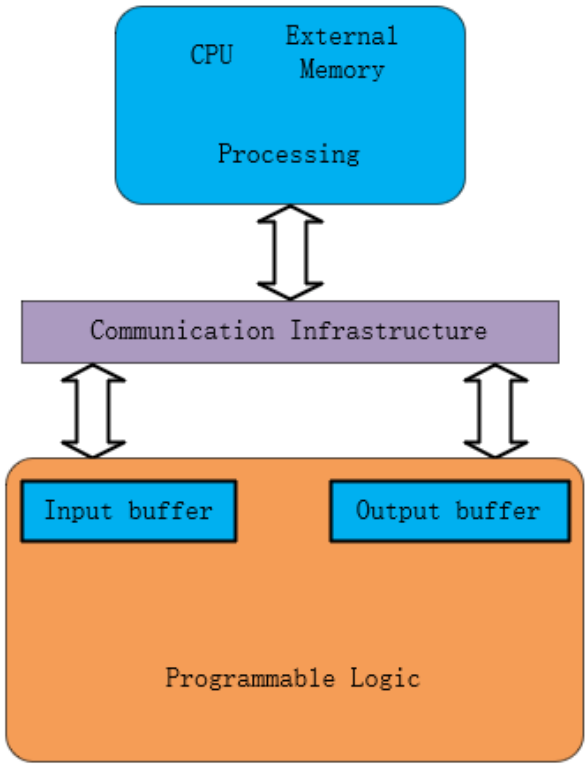

Figure 1 Logic of Data Enhancement Security Technology

3.2 Assessment of Information Security Technologies

Based on the problem analysis and requirement definition, this research will adopt the following research methodology to study and design data enhancement security strategies based on information confidentiality in the Smart IoT communication layer: in-depth analysis and assessment of possible security threats and attack methods in the Smart IoT communication layer to understand the needs and challenges in the current security environment. Evaluate existing data enhancement security strategies, analyze their applicability and limitations in Smart IoT communication layer applications, compare the security performance and efficiency of different standards, and identify their advantages and disadvantages. Through discussions with experts and case studies, the security requirements for data transmission in the Smart IoT communication layer are defined, including confidentiality, integrity, availability, authentication, and access control requirements. Based on the security threat analysis and the definition of security requirements for the communication layer, new data elevation security strategies adapted to the smart IoT communication layer are studied and designed. Symmetric boosting security algorithms, asymmetric boosting security algorithms, hash algorithms, etc., can be used to combine the characteristics and requirements of Smart IOT for innovative design. The designed data-boosting security strategy is realized by constructing an experimental environment, and performance evaluation and experimental verification are performed. Comprehensive evaluation and verification of the execution efficiency, security, and scalability of the boosted security algorithm. Perform security risk assessment of the designed data boosting security strategy, identify potential vulnerabilities and attack surfaces, and propose corresponding optimization strategies and measures to enhance the security and reliability of data transmission.

The research objective of this thesis is to propose and design a new data-boosting security strategy applicable to the communication layer of Smart IoT based on the need for information confidentiality in the communication layer of Smart IoT by evaluating and analyzing the existing boosting security algorithms. The feasibility and security of the proposed lifting security strategy in the smart IoT environment are verified through experimental validation and performance evaluation. Through these studies, the author aim to provide a secure and reliable data-boosting security policy to protect the data transmitted in Smart IoT from the risk of unauthorized access and tampering. The network security protection process, as shown in Figure 2.

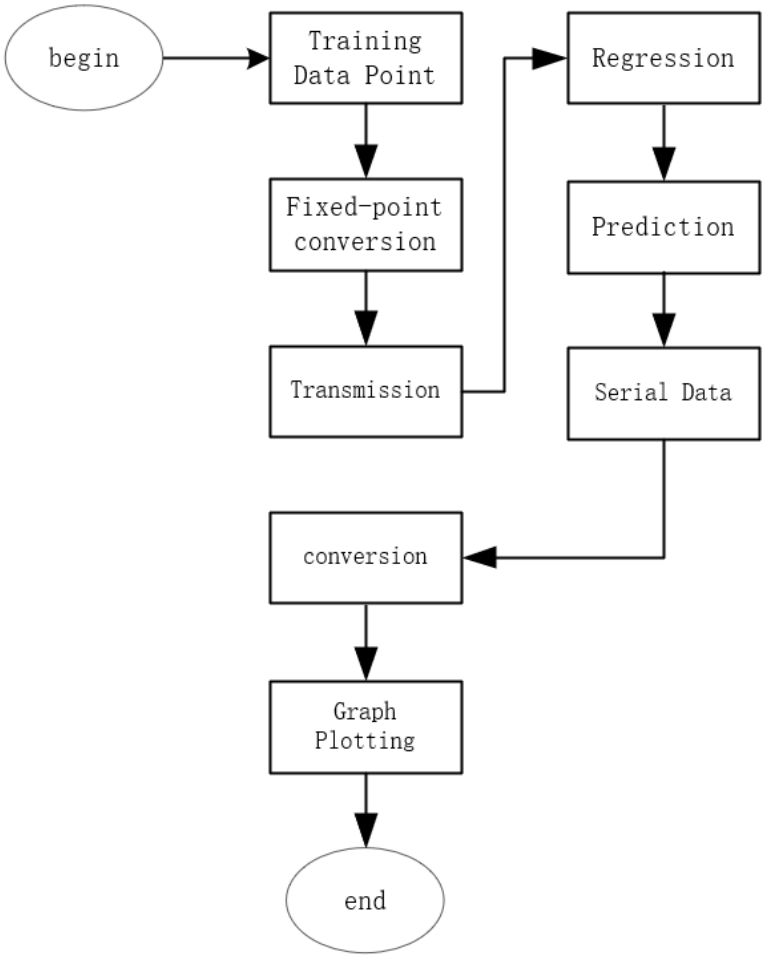

Figure 2 Network security protection process

The design of the data enhancement security policy for information confidentiality at the communication layer of Smart IoT is shown below:

$$J = \int_{t_0}^{\chi} \zeta(z(t), v(t), t)dt \tag{1}$$

J in Equation (1) is the basic idea of the data enhancement security technique to enhance the security path.

$$Z = f(z(t), v(t), t) \tag{2}$$

$$j_1 = (z_1(t_f) - 0.4) + \int_{t_0}^{\chi} (z_1^2 + u_1^2)dt \tag{3}$$

$$j_2 = (z_1(t_f) - 0.4) + \int_{t_0}^{\chi} (z_2^2 + u_2^2)dt \tag{4}$$

Z in Equation. (2) is the Z function in the network security algorithm, whose independent variable is time t; J_1 in Equation (3) is the difference function 1 of J; and J_2 in Equation (4) is the difference function 2 of J.

$$J = J_1 + J_2 \tag{5}$$

J in Equation (5) is, that is, the set of difference equations computed in this paper.

4. Results and discussion

4.1 Designs related to information confidentiality

In smart IoT applications, safeguarding information confidentiality and data enhancement security in the communication layer has become crucial. Therefore, this study aims to conduct in-depth research on information confidentiality based on the communication layer of Smart IoT and propose effective data enhancement security strategies to ensure the security of data transmission and communication security in Smart IoT systems. An extensive

literature research and review is conducted to better understand the issues of information confidentiality and data enhancement security strategies in the communication layer of Smart IoT. It examines the current smart IoT communication layer security protocols, elevated security algorithms, and related research results. The literature review found that the current research mainly focuses on protecting the confidentiality, integrity, and availability of data transmission. However, some problems and challenges were also found. First, the traditional enhancement security policies have certain limitations in the communication layer of smart IoT and cannot meet the complex smart IoT environment and requirements. Due to the special characteristics of smart IoT, it needs to cope with different network topologies, communication protocols, and device types, so it needs to design new elevated security policies in a targeted manner. Second, many devices in smart IoT are large in number and limited in resources. Therefore, efficient and lightweight elevated security algorithms need to be designed to meet the computational and storage resource constraints of smart IoT devices. In addition, devices in smart IoT systems usually have different security capabilities and computational capacities, which leads to a challenge in achieving compatibility and interoperability among devices. Consideration needs to be given to ensuring that elevated security communications between different devices can be carried out efficiently and that the security and integrity of the information are guaranteed.

Further in-depth research will be conducted to address these issues and challenges, and innovative solutions will be proposed. By proposing new elevated security policies and algorithms for the communication layer of Smart IoT, the data transmission and communication security in Smart IoT systems can be better protected. At the same time, it will continue exploring the compatibility and interoperability issues between devices to realize the overall security and sustainability of smart IoT systems. The results of this research are expected to provide strong security for smart IoT applications and contribute to building a safe and reliable smart IoT system. With the deepening of research and the further development of technology, it is foreseeable that smart IoT will be widely used in various industries and bring more convenience and security to people's lives.

To better understand the data transmission security issues in the practical applications of the communication layer of the Smart IoT, some relevant cases have been collected and analyzed. In smart IoT applications, these cases involve data leakage, tampering, replay attacks, etc.. The needs and challenges in practical applications are deeply understood by analyzing these cases. It has been found that data transmission security is crucial in smart IoT applications. For example, in smart homes, unenhanced security transmission may lead to threats to home security, and even criminals can utilize these vulnerabilities to invade home networks. In addition, in the medical field, unenhanced data transmission security may lead to leakage of patients' privacy, which poses a great risk to both patients and hospitals. The data applications of smart IoT technology (i), (ii), and (iii) are shown in Figures 3, 4, and 5.

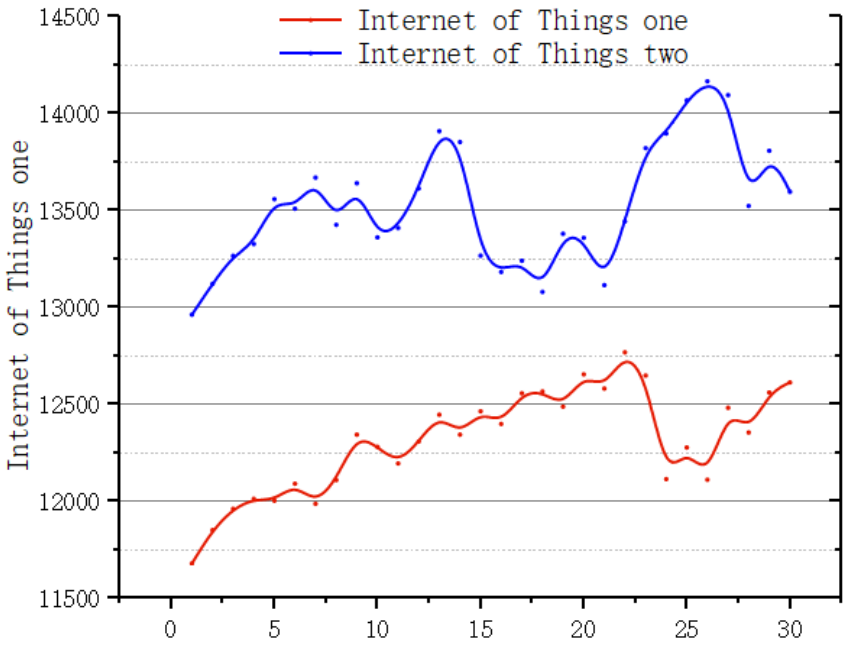

Figure 3 Data applications of smart IoT technologies (I)

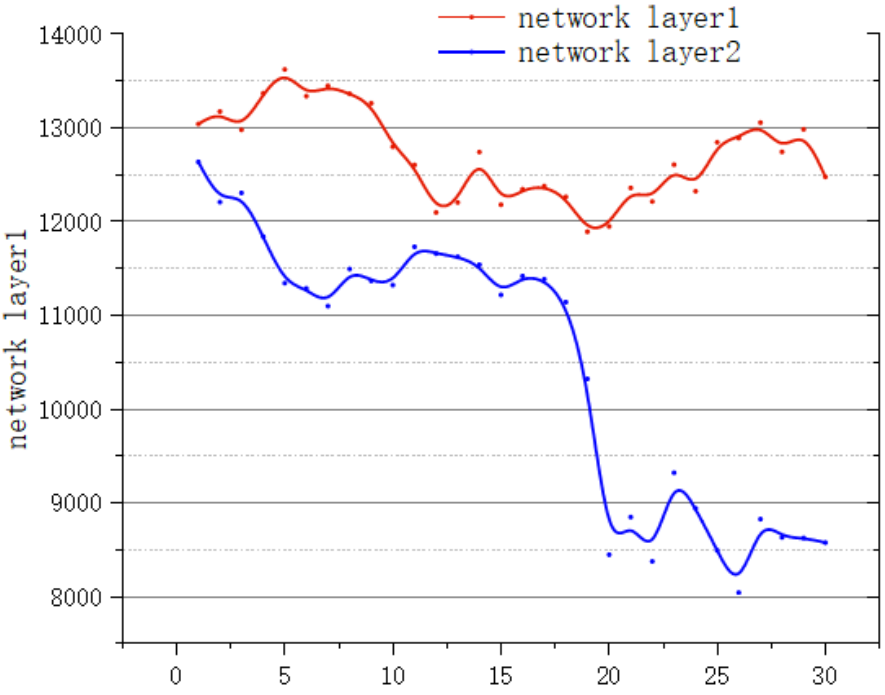

Figure 4 Data applications of smart IoT technologies (II)

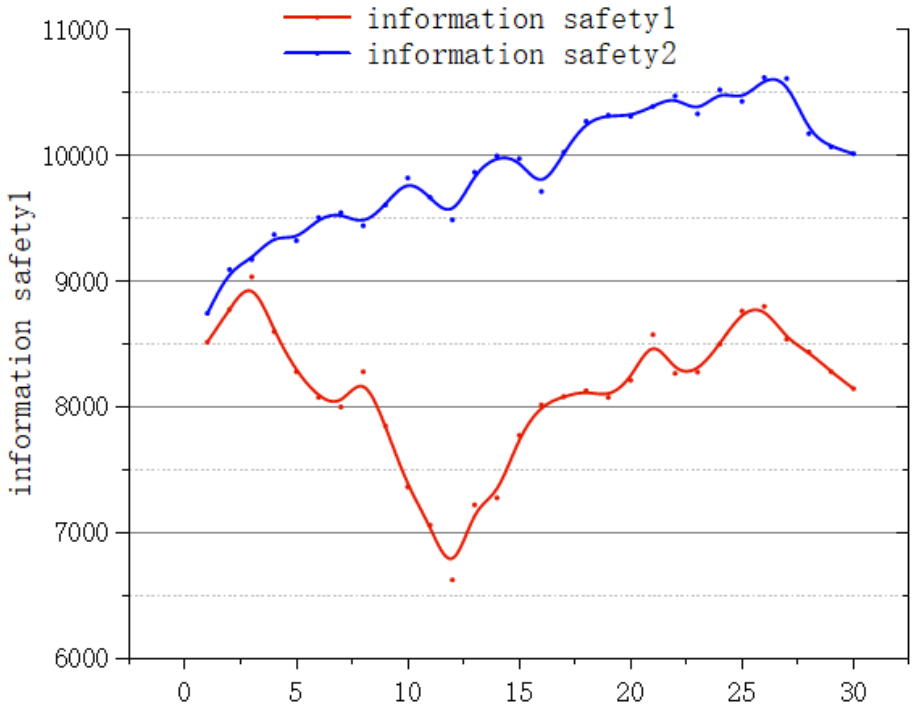

Figure 5 Data applications of smart IoT technologies (III)

To better understand the need for information confidentiality and data enhancement security strategies for the Smart IoT communication layer, interviews were conducted with several security experts in the Smart IoT communication layer, experts in enhancement security technologies, and academic experts in related fields. Valuable insights and suggestions were obtained through these interviews. Experts generally agree that data

enhancement security is key in protecting the smart IoT communication layer. They emphasized the following points: first, the elevated security algorithm should have high security and effectively resist various attacks. Second, the elevated security algorithm should have high efficiency and lightweight characteristics to adapt to the limited resources of smart IoT devices. In addition, standardized elevated security algorithms and protocols are also key, considering the heterogeneity and interoperability of devices in smart IoT systems.

Problem analysis and requirement definition were conducted by collecting and analyzing existing data. It is noted that the security threats in the smart IoT communication layer mainly include data leakage, tampering, replay attacks, etc., and the limitations of the traditional enhancement security policies are mainly reflected in the high computational complexity and high resource requirements. In addition, the requirements of the smart IoT communication layer mainly include high efficiency, lightweight, compatibility, and standardization. In summary, the research and design of data enhancement security strategies based on information confidentiality in the smart IoT communication layer must focus on improving data transmission's confidentiality, integrity, and availability. In the research, it is necessary to address the limitations of traditional boosted security policies and develop boosted security algorithms that are efficient and adaptable to the resource constraints of smart IoT devices. In addition, device compatibility and interoperability are important factors to be considered. Based on the above findings, further research and design of data-boosting security strategies for information confidentiality at the communication layer of smart IoT will be conducted. The needs and challenges in practical applications will be considered comprehensively to design elevated security algorithms and protocols that are secure and adaptable to the smart IoT environment. It is hoped that the efforts will protect the data security in the Smart IoT system and provide strong support for the sustainable development of Smart IoT.

4.2 Data Enhancement Security Policy Design

An innovative data enhancement security strategy has been developed for the smart IoT communication layer to address the current issues. The standard considers a high degree of security and possesses high efficiency and lightweight characteristics. During the design process, the characteristics and requirements of the smart IoT communication layer are deeply analyzed, and the traditional lifting security algorithm is improved and optimized. Adopting advanced lifting security algorithms and protocols significantly improves the confidentiality and secrecy of data transmission. During the design process, special attention is paid to the limited resources of smart IoT devices and their innovatively designed algorithms with low computation and low storage requirements to adapt to the requirements of different devices. This design considers the hardware limitations of the devices used in the Smart IoT environment, ensuring the efficient operation of the security-enhancing process while reducing the system's demand for computational and storage resources. To validate the practical effectiveness of its innovative design, the research team conducted a series of experiments and selected several typical application scenarios in areas such as smart homes, smart cities, and healthcare. By simulating attacks and threats in these scenarios, it could comprehensively evaluate the performance and security of its enhanced security strategy in real-world applications. The experimental results show that the innovative design can protect data transmission and communication in the smart IoT system against various attacks and threats.

The results of this research have significant innovative value and practical application prospects. The new data-enhanced security strategy provides a high degree of security while considering the resource constraints of smart IoT devices to ensure the system's efficient operation. This innovative design can be widely applied to various smart IoT scenarios to protect users' privacy and sensitive information and further promote the sustainable development of smart IoT technology. However, it is also important to realize that there are still challenges and room for improvement in practical applications. To meet the needs of the evolving smart IoT system, further optimization and improvement are needed to enhance the efficiency and performance of security algorithms. Ensuring compatibility and interoperability between devices for secure communication and data transmission is also crucial.

In conclusion, the efforts have resulted in the design of an innovative data-boosting security strategy that provides an effective solution to safeguard information confidentiality at the communication layer of smart IoT. This result shows excellent performance and security in experimental validation and has the potential to be widely applied. With further improvement and development, this research will make an important contribution to the security assurance of smart IoT systems and promote the continuous development of smart IoT technology. Iterations (i), (ii), and (iii) of the data enhancement security technique are shown in Figs. 6, 7, and 8.

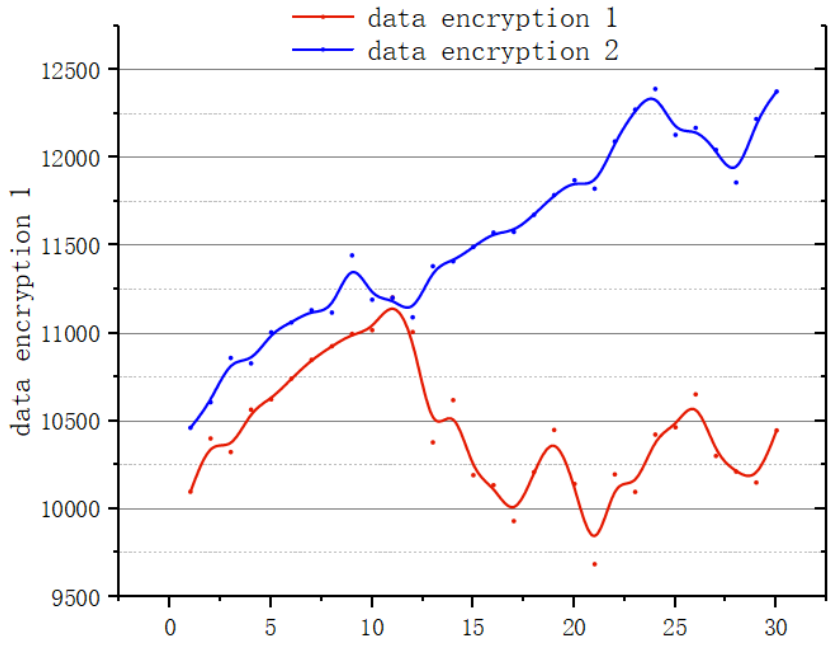

Figure 6 Iteration of data-enhanced security technologies (I)

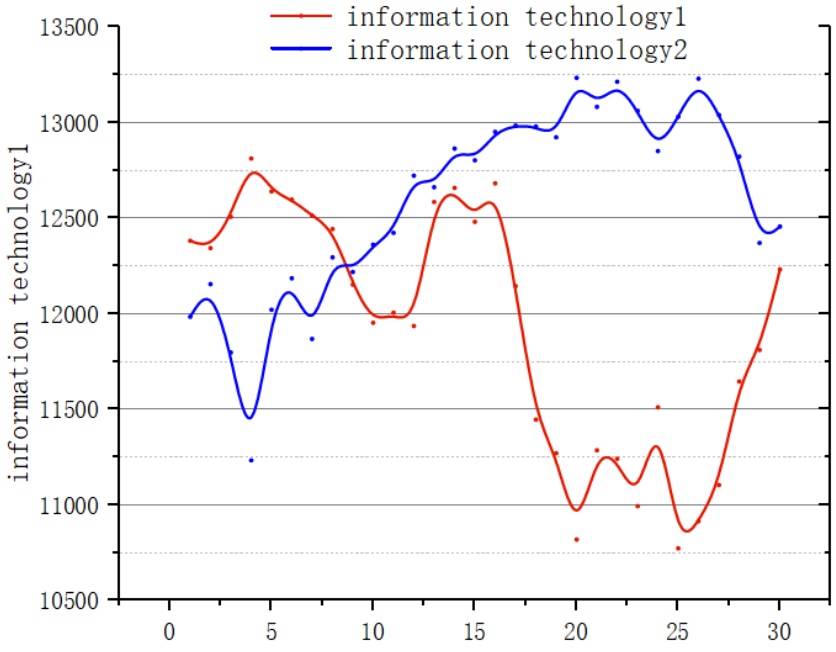

Figure 7 Iteration of Data Enhancement Security Technologies (II)

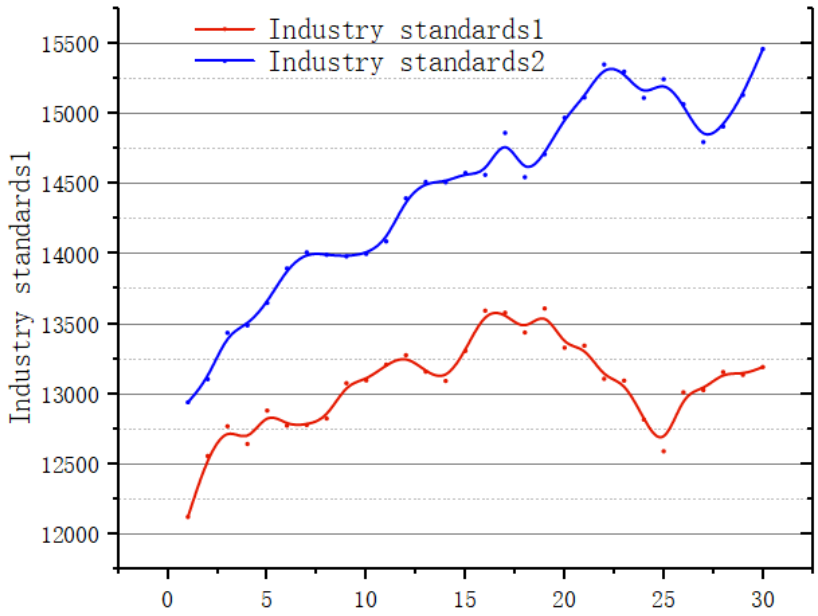

Figure 8 Iteration of Data Enhancement Security Technologies (III)

The research results have certain innovative value and practical application prospects. Firstly, the innovative data enhancement security strategy can provide high security and confidentiality and effectively defend against various attacks and threats. Second, the design balances high efficiency and lightweight characteristics and adapts to the limited resources of smart IoT devices. In addition, the enhanced security policy can be widely used in various scenarios and applications in the smart IoT domain to protect users' privacy and sensitive information. However, it is also important to recognize that there are still challenges and room for improvement in practical applications. First, further optimization and improvement are needed to enhance the efficiency and performance of security algorithms to meet the needs of increasingly complex and large smart IoT systems. Second, compatibility and interoperability between devices must be considered to enable secure communication and data transmission between devices.

To summarize, the research and innovative design of data enhancement security strategy based on information confidentiality guarantee in the communication layer of smart IoT is of great significance. Through these efforts, it proposes an innovative enhancement security strategy and verifies its feasibility through experiments. This research result not only has certain innovative value but also has a broad practical application prospect. The innovative design provides an in-depth analysis of the characteristics and requirements of the communication layer of smart IoT and improves and optimizes the traditional lifting security algorithm. Adopting advanced lifting security algorithms and protocols improves the confidentiality and secrecy of data transmission. At the same time, it also takes into full consideration the limited resources of smart IoT devices and designs algorithms with low computation and storage requirements that adapt to the requirements of different devices. To verify the effectiveness of the innovative design, a series of experiments were conducted, and several typical scenarios and applications were selected for evaluation, such as smart home, smart city, and healthcare. Simulating attacks and threats evaluates the performance and security of the innovative enhancement security policy in real-world applications. The experimental results show that the innovative design can effectively protect data transmission and communication in smart IoT systems and improve overall security. It is believed that through its efforts, it can significantly contribute to the security of smart IoT systems and promote the sustainable development of smart IoT technology. Its research results can protect users' privacy and sensitive information and provide reliable data transmission and communication security for various smart IoT application scenarios. With further improvement and development, this research will provide strong support for constructing a safe and reliable smart IoT system and promote smart IoT technology to a higher level.

5. Conclusion

This dissertation aims to study and design a data-boosting security strategy based on information confidentiality in the communication layer of the Smart IoT. By evaluating and analyzing the current data boosting security techniques for the communication layer of the Smart IoT, it is found that the existing boosting security algorithms have limitations such as high resource

consumption, insufficient security, and limited ability to adapt to the characteristics of the Smart IoT. Therefore, this thesis proposes a new data-boosting security strategy applicable to the communication layer of smart IoT and verifies its feasibility and security through experiments. The experimental results show that the proposed boosted security strategy has high efficiency and anti-attack capability while ensuring data confidentiality and integrity. The standard can meet the needs of resource-constrained devices in smart IoT and operate properly under different network topologies and scenarios of cooperative device communication. Compared with existing boosting security algorithms, this new data-boosting security strategy based on the communication layer of Smart IoT has obvious advantages in terms of performance and security. Through this study, it is fully recognized that the confidentiality of information in the communication layer of Smart IoT is crucial for the stable operation and development of Smart IoT. Data confidentiality and integrity are the keys to protecting the information transmitted in smart IoT from unauthorized access and tampering. Therefore, it is essential to study and design data enhancement security strategies applicable to the communication layer of smart IoT. The research results in this thesis are of great significance in promoting the development of information confidentiality in smart IoT. The proposed elevated security strategy provides reliable protection for data transmission in Smart IoT and helps to reduce the risk of data leakage and information tampering. This will provide higher security for smart IoT application scenarios such as smart homes, smart transportation, and industrial control systems. However, the research in this thesis has some limitations. First, due to the rapid development and diversity of smart IoT, some exceptional cases or attacks may not be covered. Therefore, further comprehensive testing and validation are needed when applying the proposed enhanced security policies to real smart IoT environments to ensure their applicability and stability. Second, with the continuous development of technology, new attack methods and security requirements may emerge; thus, long-term research and improvement are necessary. Future work can be carried out in the following aspects: further, refine and optimize the proposed enhancement security policy to improve its performance and adaptability; conduct more extensive experiments and tests to expand the coverage of samples and scenarios; and continuously track and study the cutting-edge dynamics of the information confidentiality of the Smart IoT, so that the enhancement security policy can be updated and improved in time to cope with the new threats and demands.

In summary, it is of great significance to research and design the data boosting security strategy based on the information confidentiality of the communication layer of smart IoT. This dissertation proposes a new data-boosting security strategy for the smart IoT communication layer by evaluating and analyzing the existing boosting security algorithms, and its feasibility and security are verified. The proposed standard provides a reliable guarantee for the information confidentiality of Smart IoT and supports and guides the application development of Smart IoT. Future work must further improve and optimize the enhancement security strategy to meet the evolving smart IoT needs and security challenges.

References

[1] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronicsweek*, *11*(2), 198.

[2] Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., & Arshad, H. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications*, *119*, 2603–2637. https://doi.org/10.1007/s11277-021-08348-9

[3] Ahmad, M., Riaz, Q., Zeeshan, M., Tahir, H., Haider, S. A., & Khan, M. S. (2021). Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. *EURASIP Journal on Wireless Communications and Networking*, *2021*, 1–23. https://doi.org/10.1186/s13638-021-01893-8

[4] Alavikia, Z., & Shabro, M. (2022). A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey. *Digital Communications and Networks*, *8*(3), 388–410. https://doi.org/10.1016/j.dcan.2022.01.002

[5] Azrour, M., Mabrouki, J., Guezzaz, A., & Farhaoui, Y. (2021). New enhanced authentication protocol for internet of things. *Big Data Mining and Analytics*, *4*(1), 1–9. https://doi.org/10.26599/BDMA.2020.9020010

[6] Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal*, *8*(13), 10474–10498. https://doi.org/10.1109/JIOT.2021.3062630

[7] Ferrag, M. A., Friha, O., Maglaras, L., Janicke, H., & Shu, L. (2021). Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 138509–138542.

[8] Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. *Sensors*, *21*(3), 772. https://doi.org/10.3390/s21030772

[9] Karim, A. (2022). Development of secure Internet of Vehicle Things (IoVT) for smart transportation system. *Computers and Electrical Engineering*, *102*, 108101. https://doi.org/10.1016/j.compeleceng.2022.108101

[10] Li, X., Zheng, Y., Khan, W. U., Zeng, M., Li, D., Ragesh, G., & Li, L. (2021). Physical layer security of cognitive ambient backscatter communications for green Internet-of-Things. *IEEE Transactions on Green Communications and Networking*, *5*(3), 1066–1076. https://doi.org/10.1109/TGCN.2021.3062060

[11] Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W.-C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors*, *21*(5), 1809. https://doi.org/10.3390/s21051809

[12] Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H.

(2021). Security of internet of things based on cryptographic algorithms: A survey. *Wireless Networks*, *27*(2), 1515–1555. https://doi.org/10.1007/s11276-020-02535-5

[13] Nyangaresi, V. O., Ahmad, M., Alkhayyat, A., & Feng, W. (2022). Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. *Expert Systems*, *39*(10), e13126. https://doi.org/10.1111/exsy.13126

[14] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Arshad, H., & others. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494. https://doi.org/10.1016/j.cose.2021.102494

[15] Peng, K., Li, M., Huang, H., Wang, C., Wan, S., & Choo, K.-K. R. (2021). Security challenges and opportunities for smart contracts in Internet of Things: A survey. *IEEE Internet of Things Journal*, *8*(15), 12004–12020. https://doi.org/10.1109/JIOT.2021.3074544

[16] Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings*, *80*, 3554–3559. https://doi.org/10.1016/j.matpr.2021.07.295

[17] Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of things: Security and solutions survey. *Sensors*, *22*(19), 7433. https://doi.org/10.3390/s22197433

[18] Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), 296–312. https://doi.org/10.1007/s11036-022-01937-3

[19] Sharma, R., & Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. *Transactions on Emerging Telecommunications Technologies*, *34*(11), e4571. https://doi.org/10.1002/ett.4571

[20] Wang, T., Yang, Q., Shen, X., Gadekallu, T. R., Wang, W., & Dev, K. (2021). A privacy-enhanced retrieval technology for the cloud-assisted internet of things. *IEEE Transactions on Industrial Informatics*, *18*(7), 4981–4989. https://doi.org/10.1109/TII.2021.3103547

[21] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: A comprehensive survey. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 94668–94690.