# Internet of Things Data Security Management System and Method Based on Zero Trust

Qianqian Zhang[a], Guining Geng[b], Zhiyuan Wang*[c]

[a]School of Information, Beijing Wuzi University, 321 Fuhe Street, Tongzhou District, Beijing, China 101149;
[b]Beijing Qihoo Technology corporation, 360 Digital Security Technology corporation, Building 2, Courtyard 6, Jiuxianqiao Road, Chaoyang District, Beijing, China 100015;
[c]School of Information Science and Engineering, Linyi University, West side of North Section of Industrial Avenue in Lanshan District, Linyi, China 276000

* Corresponding author:15725191054@163.com

**Abstract.** With the wide application of Internet of Things (IoT) devices and sensors, a large amount of IoT data is collected and analyzed. In the existing Internet of Things data security management technology, there is a problem that the same authentication method is adopted for the authentication information and cannot be judged according to the authentication time, which affects the authentication efficiency and data security. In order to solve these problems, a zero-trust-based IoT data security management system and method are proposed. The method includes the steps of acquiring information to be authenticated, marking authentication information, acquiring authentication times and authentication time, analyzing based on the times and time, dividing security authentication, storing authenticated information, and the like. Combined with the idea of zero trust, by storing authenticated information, the authentication process can be effectively managed, and the credibility and security of data can be improved. In the information authentication process, through verification with the stored authentication information, the number of authentications is obtained, and the security level interval is obtained according to the number of authentications and the authentication time, and then a suitable authentication scheme is selected to effectively improve the authentication efficiency.

**Keywords:** Internet of Things data security management, zero trust, security level range, authentication method

## 1 INTRODUCTION

The Internet of Things (IoT) is a new type of global network infrastructure that interconnects heterogeneous networks so that data can be collected, managed, processed, and distributed through ubiquitous devices and physical objects[1]. IoT data management is of great importance in today's digital age. With the widespread application of IoT devices and sensors, a large amount of IoT data is collected and analyzed, thereby


A. Rauf et al. (eds.), *Proceedings of the 3rd International Conference on Management Science and Software Engineering (ICMSSE 2023)*, Atlantis Highlights in Engineering 20,
https://doi.org/10.2991/978-94-6463-262-0_49

promoting the development of smart cities, smart manufacturing, health monitoring and other fields. However, in the process of IoT data management, there are some technical deficiencies that need to be resolved to improve data authentication efficiency and data security.

First of all, there is a defect in the current authentication process, that is, the same authentication method is adopted for each information to be authenticated, and different authentication methods cannot be selected based on the analysis and judgment based on the authentication information, which affects the authentication efficiency. This means that no matter what type of data or device the information to be authenticated is, it will be authenticated in the same way. This unified authentication method may lead to redundancy in the authentication process, increasing authentication time and resource overhead. Therefore, it is necessary to improve the authentication process, and select an appropriate authentication method according to the attributes, sources and security requirements of the information to be authenticated, so as to improve authentication efficiency and reduce redundancy. Secondly, there is another defect in the information authentication process, that is, in the authentication process of the same type of authentication information, the authentication process in different time periods is not considered, and it is impossible to judge and select the corresponding security authentication method according to the authentication time. This can lead to security exceptions during authentication. Due to the characteristics of IoT data, the same piece of data may have different security risks and requirements at different points in time. For example, certain data may require stricter authentication requirements during certain time periods, while simpler authentication methods may be used during other time periods. Therefore, it is very important to judge and select an appropriate security authentication method based on the authentication time to ensure the security of data at different time points.

In view of the above problems, it is of great significance to introduce zero trust as a solution. Zero trust is a security strategy and architecture. In the IoT application under the zero trust framework, the principle of "verify, never trust" should be adhered to[2], require authentication and authorization on every access request, and do not trust any user, device, or application on any internal or external network. By applying the concept of zero trust to the data management of the Internet of Things, the defects in the existing technology can be made up, and the security and authentication efficiency of the data can be improved. Combined with the idea of zero trust, this paper proposes a zero trust-based IoT data security management system and method. This method aims to solve the single problem of IoT data authentication and ensure data security. By obtaining and marking the information to be authenticated, the number of authentication times and the authentication time are obtained, and based on this information, security analysis and division of security level intervals are performed. In the information authentication process, through the verification of the authenticated information, the number of authentications is obtained, and the security level interval is obtained according to the authentication information and authentication time, and finally different authentication schemes are selected for authentication. Based on the idea of zero trust, this method introduces a variety of authentication methods and authentication that considers time changes, as well as the division of security level intervals, effectively solving the

problem of single data authentication in the Internet of Things, and improving data security and authentication efficiency.

## 2 Related Work

In the prior art, there are some defects and challenges in the data management process of the Internet of Things, which need to be solved and improved. In order to solve the privacy and security issues in IoT data management, Jiang[3] et al. proposed a cross-chain framework to achieve efficient and secure IoT data management by integrating multiple blockchains. The framework uses the consortium blockchain as the control site, while using other blockchain platforms customized for specific IoT scenarios as the support for all IoT devices. In this way, off-chain channels are opened on the consortium blockchain, and transactions in these channels are merged for confirmation using the notarization mechanism. Bassirou Diène[4] et al. proposed a solution for IoT data management to address challenges such as diversity, heterogeneity, and large data volumes, adopting a middleware or architecture-oriented approach to integrate the generated data, and Provides solutions for efficiently storing, indexing, and processing structured and unstructured data, as well as support for NoSQL languages. Kamalendu Pal[5] et al. proposed a blockchain-based IoT application architecture, aiming to solve the current data isolation problem in the IoT, especially in the supply chain network in the textile and apparel industry. The architecture supports transaction services across multi-participating clothing enterprise supply chain networks through distributed data management. Through the use of radio frequency identification (RFID) tags and a sensor-based data communication network, the architecture is able to capture real-time information from different parts of the textile and apparel manufacturing value chain. Muhammad Saqlain[6] et al. proposed an IoT-based industrial data management system (IDMS) framework, which aims to solve the challenges of large-scale, heterogeneous, and time-sensitive IoT data management. Provide users with a service-oriented architecture through five basic layers consisting of physical layer, network layer, middleware layer, database layer and application layer. Olivier Debauche[7] et al. proposed a new distributed edge architecture (SSCIoT), which aims to realize IoT data management and improve the efficiency of data transmission by establishing short supply chain circuits between data generators and users. Melanie Lourens[8] and others aimed at the diversity, heterogeneity and mass of data generated in the Internet of Things, and the traditional database management system is no longer applicable. Through the second qualitative analysis, it focuses on the database management and its challenges in the IoT technology, and proposes special solutions for the data management of the Internet of Things. Krishna Kumar Vaithinathan[9] and others discussed the importance of combining blockchain, artificial intelligence and the IoT in the data management of the Internet of Things, focusing on the integration of these three technologies for improving privacy, scalability, The impact of automation on security, authentication, and business data models, and offers a variety of converged use cases.

Based on the above related work in the field of IoT data management, there is still a major problem that is the singleness of IoT data authentication. Existing methods often

only rely on a single authentication method and lack the ability to comprehensively consider different authentication factors, resulting in the limitation of the efficiency and accuracy of the authentication process. In order to solve this problem, a zero-trust based IoT data security management system and method is proposed, which provides a more comprehensive and reliable IoT data authentication scheme by comprehensively considering the number of authentications, authentication time and security level. It overcomes the limitation of a single authentication method in the existing methods, and improves authentication efficiency and data security.

# 3 Related Technology Introduction

## 3.1 Zero Trust

Zero trust is an innovative concept of network security protection, introduced by Kindervag[10] in 2010. In 2011, Google began to build the BeyondCorp project based on the zero trust concept[11]. In 2020, NIST [12] gave the definition of zero trust. Its core principle is to abandon the default trust, based on continuous verification and never trust. To put it simply, zero trust is not to easily trust any person, device or system inside or outside the enterprise network, but to rebuild the trust basis of access control through identity authentication and authorization. The purpose of this is to ensure the trustworthiness of identities, devices, applications and links, thereby improving overall network security.

The traditional security model usually establishes a boundary protection within the enterprise network, places trust within the network boundary, and once authenticated, internal resources can be freely accessed. However, there are many potential security risks with this model because once attackers successfully penetrate the perimeter protection, they are able to move freely within the internal network. The concept of zero trust is to change this traditional model, reduce the scope of trust to the minimum, and verify it in each access request.

Based on the principle of zero trust, the office system can achieve security in three key aspects:

Endpoint security: In a zero trust model, every endpoint device is considered untrustworthy, whether it is inside or outside the corporate network. Terminal devices need to go through strict authentication and authorization before they can gain access to internal resources. In addition, endpoint devices should have security patches and protections against potential threats and attacks.

Link security: In the zero trust model, all network links are regarded as untrustworthy, whether it is the internal LAN of the enterprise or the external Internet. Data transmission requires the use of security mechanisms such as encryption and authentication to ensure the confidentiality and integrity of data during transmission. Additionally, network traffic monitoring and intrusion detection systems can help spot and block potential cyber attacks.

Access control security: The access control under the zero-trust model is very strict, each user and device needs to be authenticated, and can only obtain access with the least privilege. Zero trust-based access control combines fine-grained permission

assignment with continuous verification to ensure that only authorized users and devices can access sensitive data and resources. Additionally, behavioral analytics and threat intelligence can help detect and block unauthorized access and anomalous behavior.

In general, an office system based on the principle of zero trust can protect the security of terminal devices, network links, and access control in a more cautious and meticulous manner. Through the principles of continuous verification and never trust, the risk of security breaches can be reduced, and a more reliable protection mechanism can be provided to adapt to increasingly complex and changing security threats.

### 3.2 IoT Data Security Management

IoT data security management refers to a series of measures and methods for data protection and management in the IoT environment. Due to the particularity of the Internet of Things, the data involved are extensive, real-time and sensitive, so the security management of the IoT data is very important.

The following is an introduction to the relevant knowledge of IoT data security management:

Authentication and authorization: Devices and users in the IoT need to be authenticated and authorized to access and operate data. Authentication verifies the identity of a device or user, while authorization determines its authority to access and manipulate data. Effective authentication and authorization mechanisms can ensure that only legitimate entities can access and use IoT data.

Encryption and decryption: IoT data needs to be encrypted during transmission and storage to prevent unauthorized access and theft. Encryption technology converts data into an unreadable form that only authorized entities can decrypt and restore the data. Common encryption algorithms include symmetric encryption and asymmetric encryption.

Integrity protection: The integrity of IoT data means that the data has not been tampered with or damaged during transmission and storage. In order to ensure the integrity of the data, digital signatures and hash algorithms can be used to verify the integrity of the data. Once the data is tampered, its hash value will change, so that the tampering of the data can be detected.

Auditing and monitoring: The security management of IoT data requires real-time auditing and monitoring in order to discover and respond to potential security threats and abnormal behaviors in a timely manner. By monitoring the access and usage of data, abnormal behaviors can be detected in time and corresponding measures can be taken to deal with them.

Security policies and policies: Developing and enforcing appropriate security policies and policies is crucial for the secure management of IoT data. Security policies and policies should include regulations on data access control, encryption requirements, authentication requirements, security audit requirements, etc., to ensure that IoT data is effectively protected and managed.

The goal of IoT data security management is to protect the confidentiality, integrity, and availability of IoT data and prevent unauthorized access, tampering, and

destruction. Comprehensive security management of IoT data can be achieved through effective authentication, encryption, integrity protection, auditing and monitoring, and security policies and policies.

# 4 Internet Of Things Data Security Management System And Method Based On Zero Trust

This paper proposes a zero-trust-based IoT data security management system and method, which includes a network receiving terminal, a network analysis terminal, a network authentication terminal and a server. It improves the efficiency of certification by obtaining the information to be certified in the IoT and marking it, analyzing it and dividing it into security certification. The method stores the authenticated information, divides the security level intervals according to the authentication times and time, and selects different authentication schemes for authentication, which provides an effective security management method.

## 4.1 IoT data security management system based on Zero trust

1)System model

The security management system includes a network receiving terminal, a network analyzing terminal, a network authenticating terminal and a server as shown in Figure 1. The network receiving terminal is responsible for obtaining the IoT information to be authenticated and sending it to the network authentication module. The network analysis terminal is used to mark authentication information, analyze authentication times and time, and divide security level intervals. The network authentication terminal is used to confirm the information to be authenticated, encrypt the authentication scheme, and verify according to the security level interval.

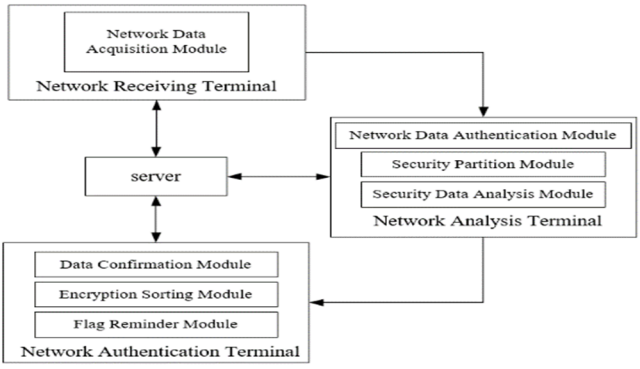


**Fig. 1.** Overall system block diagram of IoT data security management system based on zero trust

The network receiving terminal has a network data acquisition module, which is used to obtain information to be authenticated by the Internet of Things. The network data acquisition module is connected to a storage unit, and the storage unit stores the authenticated information. The stored information includes the IP address of the authentication information, the user Name, obtain the information to be authenticated by the IoT and transmit it to the network authentication module.

The network analysis terminal includes a network data authentication module, a security data analysis module and a security division module. The network data authentication module marks the authentication information, and obtains the authentication times and authentication time of the authentication information after the authentication. The security data analysis module conducts analysis based on the authentication times and authentication time to obtain the security analysis content. The security division module receives the security analysis content, and performs security authentication division, and divides different security level intervals. According to the requirements of the information to be authenticated, a corresponding security authentication scheme is set.

The network authentication terminal includes a data confirmation module, an encryption sorting module and a mark reminding module. The encryption sorting module encrypts the security authentication scheme according to the security level interval. The data confirmation module confirms the received information to be authenticated, and obtains the security level range of the scheme to be authenticated. Verify and confirm according to the security level interval. If the verification is passed, the server will pass the verification of the received information to be verified. If the verification is not passed, the marking and reminding module marks the information to be certified and issues a reminding instruction. The server rejects the information authentication according to the reminder instruction for the information to be authenticated.

This system structure can realize the security management and authentication of IoT data, and ensure the credibility and security of IoT data through the acquisition, analysis, and division of authentication information, as well as the selection and verification of authentication schemes based on security level intervals.

2)Security model

IoT data may face various forms of attack threats. Attackers may steal, tamper or forge IoT data through various means, resulting in data unreliability and security issues. Attackers can be insiders, external hackers, competitors, or other malicious entities.

Specifically, the following are some possible forms of attack:

Data theft attack: Attackers try to obtain sensitive data transmitted by the IoT, such as personally identifiable information, confidential business data, etc. This may lead to issues such as privacy leaks and commercial secret leaks.

Data Tampering Attacks: Attackers attempt to tamper with IoT data and modify its contents for purposes of deception, misleading, or destruction. This can lead to wrong decisions, damage to the reputation of the business, or financial loss.

Identity forgery attack: An attacker impersonates a legitimate user or device to gain unauthorized access, operation, or transmission by forging an identity. This could lead to unauthorized data access, service misuse or system breakdown.

Replay attack: An attacker intercepts legitimate data streams and resends them at a later time to trick the system. This can lead to duplicate operations, inconsistent data, or misleading results.

Denial of service attack: An attacker attempts to overload or destroy system resources so that it cannot work normally, resulting in unavailable services. This can lead to production interruptions, business interruptions, or compromised user experience.

3)Design goals

The design goal of this zero trust-based IoT data security management system is to provide a solution to the aforementioned IoT data security challenges. The system is designed to achieve the following design goals:

Data acquisition and authentication: The system obtains the IoT data to be authenticated through the network receiving terminal and the network authentication terminal, and marks the authentication information. Through the data confirmation module and the encryption sorting module, the authentication information is verified and confirmed to ensure the integrity and credibility of the data.

Security data analysis and division: The network analysis terminal of the system includes a security data analysis module and a security division module. The security data analysis module analyzes the data based on the authentication times and authentication time, and extracts the security analysis content. The security division module receives the security analysis content, and divides the security certification according to the security level interval to ensure that the data is properly certified under different security levels.

Storage and management: The system stores and manages the authenticated information through the database layer. The storage of authentication information enables the system to verify and compare with the stored authentication information during the information authentication process, improving the accuracy and efficiency of authentication.

To sum up, the IoT data security management system based on zero trust aims to provide more reliable and secure data authentication and management through comprehensive data acquisition, authentication, analysis and storage management mechanisms. The design goal of the system is to protect the security and reliability of IoT data, effectively deal with various attack forms, and provide security guarantee for IoT applications.

### 4.2 IoT data security management method based on Zero trust

This method aims at the problems of unified authentication mode and the inability to judge according to the authentication time in the existing IoT data security management technology. By comparing the authentication information with the stored information, the authentication information is marked and the authentication times and authentication time are obtained. Analyze based on the number of times and time, divide the security level interval, and select the appropriate authentication scheme according to the security level interval. Improve authentication efficiency and data security by verifying confirmation and reminding rejection.

The specific steps of the method are shown in Figure 2, and the specific steps are as follows:

Step 1: Compare the information to be authenticated with the stored information. If the same stored authentication information appears, the received information will be defined as the record verification information. If the same stored authentication information does not appear, the received information will be defined as the initial verification. The information defines the record verification information and the initial verification information as the information to be authenticated, and obtains the information to be authenticated in the Internet of Things.

Step 2: mark the authentication information, and obtain the authentication times and authentication time of the authentication information after marking.

The specific steps to obtain the authentication times and authentication time are as follows:

Step 2.1: Acquire the record verification information in the information to be verified, mark it as type a, and mark it as $a_1$, $a_2$… $a_{z1}$ respectively, obtain the initial verification information in the information to be verified, and mark it as type b, respectively marking it as $b_1$, $b_2$…$b_{z2}$.

Step 2.2: Obtain the number of authentication times and authentication time of type a marking in the T time period and in the storage unit. Acquire the authentication times and authentication time of type b marking in the T time period.

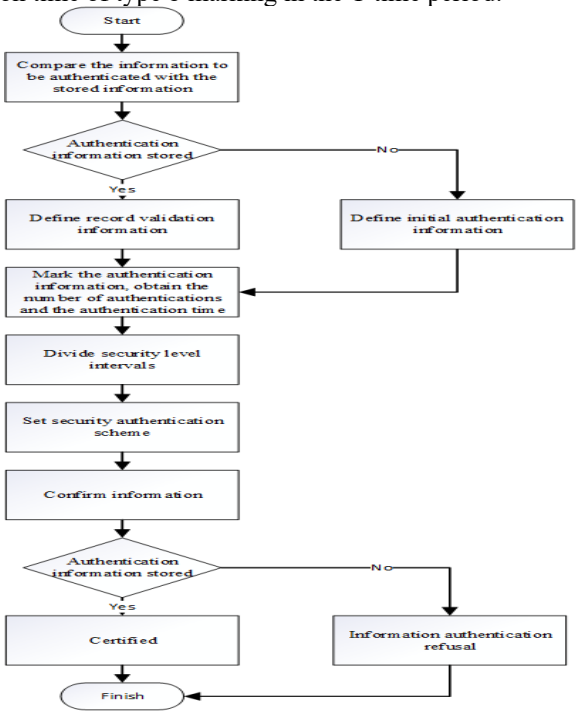


**Fig. 2.** Step diagram of IoT data security management method based on zero trust

Step 2.3: Acquire the number of authentications marked $a_1$, and the number of authentications obtained is $c_1$. The number of authentications marked az1 is obtained, and the number of authentications obtained is $c_{z1}$, The number of authentications marked b1 is obtained, and the number of authentications obtained is obtained. The number of times is $d_1$, and the number of authentications marked $b_{z1}$ is obtained, and the number of authentications obtained is $d_{z1}$.

Step 2.4: Arrange in descending order according to the number of authentications obtained, and set the first authentication interval, the second authentication interval, and the third authentication interval according to the order of arrangement.

Step 2.5: Acquire the authentication time corresponding to each authentication times obtained, set the authentication time interval according to the authentication time, set [8:00, 12:00], (12:00, 18:00), [18 :00, 24:00], (0:00, 8:00) is the authentication time interval, count the times of authentication time in each authentication time interval, arrange the counted times in descending order, and follow the time with the most times The interval to the time interval with the smallest number of times is divided into a first time interval, a second time interval, a third time interval and a fourth time interval in sequence.

Step 3: Analyze based on the number of authentication times and authentication time to obtain the security analysis content, receive the security analysis content to divide the security authentication, and divide the security level interval.

When dividing the security level interval, the specific steps are as follows:

Step 3.1: The security analysis module receives the number of authentications and the authentication time, obtains the authentication interval of the authentication times, and obtains the time interval of the authentication time.

Step 3.2: Obtain the safety certification reference value by analyzing the certification interval and time interval. When obtaining the safety certification reference value, the details are as follows:

Assign k to the authentication interval, assign $k_1$ to the first authentication interval, assign $k_2$ to the second authentication interval, assign $k_3$ to the third authentication interval, assign kl to the time interval, assign $k_{l1}$ to the first time interval, and assign $k_{l1}$ to the second time interval The value is assigned to $k_{l2}$, the third time interval is assigned to $k_{l3}$, and the fourth time interval is assigned to kl4.

Set the security authentication reference value to *aqz*. It obtains the security authentication reference value through the authentication interval assignment combined with the time interval assignment.

The calculation of the safety certification reference value is shown in formula (1).

$$aqz = k \times k_l \tag{1}$$

When performing specific calculations, replace k with $k_1$, $k_2$ or $k_3$ according to the certification interval of the number of certifications, and replace $k_l$ with $k_{l1}$, $k_{l2}$, $k_{l3}$ or $k_{l4}$ according to the time interval of the certification time.

Step 3.3: Arrange the safety certification reference values in ascending order, and set the first security level interval, the second security level interval, and the third security level interval according to the order of arrangement. The security of the first security level interval is greater than that of the second security level interval. The

security of the second security level interval is greater than the security of the third security level interval.

Step 4: Set the security authentication scheme according to the security level interval of the obtained information to be authenticated. If it is the first security interval, set the first authentication scheme. Through verification of SMS, verification of ID number and face verification Composition encryption. If it is the second security zone, set the second authentication scheme, and verify the SMS and verify the ID number to form encryption together. If it is the third security zone, set the third authentication scheme, and verify it through the SMS verification encryption. Encrypt the security authentication scheme according to the security level interval.

Step 5: In the process of confirming the information to be authenticated, the data confirmation module confirms the received information to be authenticated, obtains the security level interval of the scheme to be authenticated, and performs verification and confirmation according to the security level interval. If the information to be authenticated passes the authentication, if the confirmation fails, the marking reminder module will mark the information to be authenticated, send a reminder instruction, and the server will reject the information authentication of the information to be authenticated according to the reminder instruction.

This method unifies the authentication method and authentication time judgment, improves authentication efficiency, enhances data security through security level intervals and different authentication schemes, and adopts the concept of zero trust to continuously verify that no one, device, or system is trusted, improving the overall security.

### 4.3 Security Analysis

The system and method take a number of measures to ensure the integrity, credibility and confidentiality of the IoT data, provide a reliable security authentication mechanism to prevent malicious attacks and data tampering, thereby ensuring the safe operation and reliability of the IoT environment. Continuous development. The following is a detailed analysis of the security of the system and method:

Data acquisition and authentication security: The network receiving terminal obtains the IoT information to be authenticated through the network data acquisition module. This module ensures that the source of the data is credible, and records the number of certifications and certification time by marking the certification information, so as to track and verify the authenticity of the data.

Data analysis and division security: the network analysis terminal includes a security data analysis module and a security division module. The security data analysis module analyzes the data based on the authentication times and authentication time, and generates security analysis content. The security division module receives the security analysis content, and divides and authenticates the data according to the security level interval. The work of these modules ensures the trustworthiness and integrity of data while strengthening the protection of data at different security levels.

Data confirmation and encryption sorting security: the network authentication terminal includes a data confirmation module and an encryption sorting module. The data confirmation module confirms the received information to be authenticated, and obtains

the security level range of the scheme to be authenticated. Verify and confirm according to the security level interval, if the verification is passed, the server passes the verification, otherwise, the marking and reminding module marks the information to be certified and sends a reminding command. The encryption sorting module encrypts the authentication scheme according to the security level interval to ensure the confidentiality and security in the authentication process.

Storage and verification security: the system is based on the storage of authenticated information and verification with the stored authentication information. By comparing with the stored authentication information, verify the authentication times of the authenticated information, and obtain the security level interval according to the authentication information and authentication time. Select a suitable authentication scheme for authentication according to the security level interval, and improve the reliability of the authentication process.

Through the above security measures, the system and method can protect the integrity, credibility and confidentiality of the IoT data. It provides a reliable security authentication mechanism, prevents malicious attacks and data tampering, and ensures the safe operation and sustainable development of the IoT environment. These security measures together constitute a comprehensive security management system and method, which effectively guarantees the security and reliability of IoT data.

## 5 Conclusions

In this paper, aiming at the defects in the management process of IoT data, combined with the idea of zero trust, a zero-trust-based IoT data security management system and method are proposed. Through the acquisition and marking of authentication information, as well as the analysis of authentication times and authentication time, the security analysis content is obtained and the security authentication is divided, and different security level intervals are divided. In addition, the authenticated information is used for storage and verified with the stored authentication information during the information authentication process. By obtaining the authentication times of the authentication information and obtaining the security level interval according to the authentication information and the authentication time, an appropriate authentication scheme can be selected for authentication, avoiding the dependence on a single authentication method, thereby improving the authentication efficiency. It provides strong support for the reliability and trustworthiness of IoT data by improving authentication efficiency and data security.

## Acknowledgment

This work is partially funded by the University-Enterprise Cooperation Fund Project(5GRHBYJS). We also thank the anonymous reviewers for many valuable comments.

## REFERENCES


1. Sadeghi-Niaraki A. Internet of Thing (IoT) review of review: Bibliometric overview since its foundation[J]. Future Generation Computer Systems, 2023, pp. 361-377.
2. Wang J, Chen J, Xiong N, et al. S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT[J]. ACM Transactions on Internet Technology, 2022. doi: https://doi.org/10.1145/3511902.
3. Jiang Y, Wang C, Wang Y, et al. A cross-chain solution to integrating multiple blockchains for IoT data management[J]. Sensors, 2019, 19(9): 2042. doi: https://doi.org/10.3390/s19092042.
4. Diène B, Rodrigues J J P C, Diallo O, et al. Data management techniques for Internet of Things[J]. Mechanical Systems and Signal Processing, 2020, 138: 106564. doi: https://doi.org/10.1016/j.ymssp.2019.106564
5. Pal K. IoT and blockchain technology in apparel manufacturing supply chain data management[J]. Procedia Computer Science, 2020. 170: 450-457.
6. Saqlain M, Piao M, Shim Y, et al. Framework of an IoT-based industrial data management for smart manufacturing[J]. Journal of Sensor and Actuator Networks, 2019, 8(2): 25. doi: https://doi.org/10.3390/jsan8020025
7. Debauche O, Mahmoudi S, Guttadauria A. A new edge computing architecture for IoT and multimedia data management[J]. Information, 2022, 13(2): 89. doi: https://doi.org/10.3390/info13020089
8. Lourens M, Tamizhselvi A, Goswami B, et al. Data6ase Management Difficulties in the Internet of Things[C]//2022 5th International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2022: 322-326.
9. Vaithinathan K K, Parthiban L. Data Management and Industries Automatization Using Blockchain, AI, and IoT[M]//The Convergence of Artificial Intelligence and Blockchain Technologies: Challenges and Opportunities. 2022: 43-68.
10. Osborn B, McWilliams J, Beyer B, et al. Beyondcorp: Design to deployment at google[J]. 2016.
11. Ward R, Beyer B. Beyondcorp: A new approach to enterprise security[J]. Login the Magazine of USENIX and Sage. 39(6) (2014) 6-11.
12. Rose S, Borchert O, Mitchell S, et al. Zero trust architecture[R]. National Institute of Standards and Technology, 2020. doi: https://doi.org/10.6028/NIST.SP.800-207.