Authentication and Data Protection Mechanism in IoT Devices

Zhang Yule
Forensics & Cybersecurity Research Center
Asia Pacific University of Technology & Innovation
Kuala Lumpur, Malaysia
tp084891@mail.apu.edu.my

Dr. Julia Juremi
Forensics & Cybersecurity Research Center
Asia Pacific University of Technology & Innovation
Kuala Lumpur, Malaysia
julia.juremi@mail.apu.edu.my

Kazi Farhan Ishraq
Forensics & Cybersecurity Research Center
Asia Pacific University of Technology & Innovation
Kuala Lumpur, Malaysia
tp072329@mail.apu.edu.my

***Abstract*— Due to the rapid development of Internet of Things (IoT) technology, it is becoming more frequently used in everyday life and industrial applications. While these devices provide great convenience in our daily lives, they are also subject to serious security threats, including malware infections, DDoS attacks, data theft, identity theft, man-in-the-middle attacks, physical security threats, firmware vulnerabilities, lack of authentication and encryption, supply chain attacks, and user errors. These threats make the devices vulnerable to attacks leading to data leakage and service disruption.**

The aim of this paper is to analyze the authentication and data protection mechanisms in IoT devices and to explore the current challenges and feasible solutions. It is shown that improved authentication mechanisms can significantly increase the security of devices and thus better protect user privacy. Finally, the paper also presents suggestions and directions for future research.

Keywords*— *Internet of Things (IoT), Authentication, Data Protection

I. RESEATCH BACKGROUND

In recent years, with the continuous development of information technology in China, big data technology has been widely used in many fields, such as family, medical, industry, etc., especially in the computer industry, which reflects high value and can promote the continuous development of computer technology. However, in the context of the development of the big data era, there are many problems in computer network security, such as the spread of network viruses, hacker attacks, phishing sites, etc., which all affect the operational security of the computer network system, and effective measures need to be taken to prevent them so that the computer network security can be effectively guaranteed. Through the exploration of computer network security precautions, it is conducive to put forward some reliable reference basis to promote the effective work of computer network security, especially in the authentication and access control.

II. PURPOSE AND SIGNIFICANCE OF THE STUDY

First, by ensuring that only authenticated users and devices can access IoT devices, the security of the devices can be significantly improved, reducing the risk of unauthorized access and data leakage. Second, IoT devices involve many sensitive user data, so enhanced authentication and access control can do a good job of protecting this data, maintaining its confidentiality and integrity, and preventing malicious tampering or leakage of information. In addition, enhanced security can increase users' trust in devices and services so that IoT technologies can be more widely used. Effective authentication and access control mechanisms can also reduce the occurrence of security incidents, minimize economic losses and brand reputation damage due to security breaches, and safeguard an organization's business interests. In addition, research and development of new authentication and access control technologies will lead to the development of the entire technology field and promote the convergence of emerging technologies (e.g., artificial intelligence and blockchain). Therefore, studying this topic has important theoretical value and practical significance

III. LITERATURE REVIEW

Zang Jingsong (2010) points out that in addition to the traditional network security issues, the Internet of Things has some special security issues that are different from each other, which are mainly manifested in the following aspects: (1) As the Internet of Things requires wireless transmission on many occasions, if the signal exposed in the public place is not protected, the information can be easily stolen, and at the same time, it is easy to be interfered with, which will have a direct impact on the security of the Internet of Things. Moreover, because IoT applications can replace people to complete some complex and dangerous work, most of the IoT machines are deployed in unmonitored places, it is easy to be damaged by attackers, and even through the local operation to replace the machine's hardware and software. (2) Transmission and information security of the core network. Although the core network has a relatively complete security protection capability, due to the huge number of nodes in the Internet of Things, it still exists in clusters, so it will lead to service attack failure due to a large number of machines sending data to clog the network during data dissemination. (3) Security of IoT business. Since IoT devices may be deployed first and then connected to the network, and there is no one to monitor the IoT nodes, how to configure IoT devices with remote signing information and service information becomes a challenge. The huge and diverse IoT platform needs a powerful and unified security management platform; otherwise, the independent platform will be overwhelmed by a wide variety of IoT applications, which makes how to manage security information such as logs of IoT machines a new problem, and it is likely to destroy the trust relationship between the network and the business platform, leading to a new round of security problems.

Tan Chen's (2020) paper analyzes 2 commonly used schemes for IoT authentication at present: (1) On the basis of public key infrastructure (PKI), authentication schemes require strong specification of verification signatures; even if the message is leaked in the transmission process, it can still achieve secure and unique authentication. 2) In the authentication scheme based on the certificate-less signature (CLS, the certificateless signature), the key generation center (KGC, the key generation center) is based on the identity identification number (ID, the certificateless signature) of the IoT device. CLS, the certificateless signature) authentication scheme, the key generation center (KGC, the key generation center) according to the IoT device identity identification number (ID, identity document) to generate the corresponding part of the private password, the device uses the secret value and part of the private key to generate the actual private key. The device uses the secret value and the partial private key to generate the actual private password.
Guo, Y., Guo, Y., Xiong, P., Yang, F., & Zhang, C. (2024) points out that the wide application of IoT devices poses serious challenges in terms of security. The current authentication schemes in the IoT environment have many limitations and are not able to effectively cope with these challenges. With the limited resources of IoT devices, the complex and changing network environment, and the wide range of attack surfaces, it is difficult for traditional authentication mechanisms to meet the security requirements. In addition, the heterogeneity and dynamics of IoT systems also increase the complexity of security issues. Therefore, it is necessary to develop a more secure and reliable authentication mechanism according to the characteristics of the IoT environment to maintain the security of the whole IoT system environment. This requires further research and innovation, including the use of emerging technologies such as blockchain and quantum cryptography to improve the security of IoT authentication. Only in this way can we effectively deal with the increasing security challenges in the IoT environment.

IV. METHODS AND TECHNIQUES

A. Design of authentication mechanisms

Multi-factor authentication (MFA) is an authentication method that provides higher security by requiring the user to provide two or more different types of credentials, such as knowledge factors (e.g., passwords), ownership factors (e.g., cell phones, cards), and biometric factors (e.g., fingerprints, facial recognition). Compared with single-factor authentication (SFA), MFA can better protect computing devices and avoid unauthorized access to critical services. In the traditional MFA approach, the system key S is usually "split" and distributed to a group of key holders. A Lagrangian interpolation formula is then used to recover the key S. A high-tech enterprise uses multiple systems internally, and each account system has different security level requirements for passwords. When switching between different systems, employees need to authenticate several times, and if the authentication is unsuccessful, they have to find the IT department to change their passwords, resulting in poor experience and greatly affecting work efficiency. After deploying MFA, user identity can be verified before logging into programs or networks with strict privileges, which, together with Single Sign-On (SSO), enables seamless access to multiple applications and improves the productivity of employees and IT. However, this approach is not applicable to MFA scenarios, as the biometric parameters are already in place and it is not possible to assign new key shares or modify them (Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. 2018). In addition to shielding sensitive biometric data from disclosure, the technique can nevertheless authenticate individuals in the event that certain requirements are not met or information is inconsistent. Unfortunately, there are a number of drawbacks to using passwords as a traditional authentication method. These include security concerns like password leakage and easy cracking; usability issues like the strain on users' memory and the inconvenience of having to reset passwords often, which can be unsettling to users; management issues like the high cost of password database maintenance and the difficulty of enforcing password policies; privacy issues like the potential for password misuse; and scaling issues like the difficulty of adjusting to new security requirements.

Blockchain is a distributed ledger technology derived from the digital cryptocurrency Bitcoin. Blockchain has the advantages of decentralization, de-trust, anonymity, and data immutability, breaking through the limitations of traditional centralized technologies. Blockchain technology supports device expansion, which can be used to build efficient and secure distributed IoT networks, as well as to deploy data-intensive applications running in massive device networks, and can provide a trust mechanism for IoT to safeguard the trustworthiness, reliability, and transparency of ownership and transaction records. At the same time, blockchain technology can provide a guarantee mechanism for user privacy, thus effectively solving the data management, security, and privacy issues brought about by centralized IoT and pushing IoT to evolve towards the advanced form of home intelligence. Combining blockchain and IoT is a development trend, and the distributed characteristics of blockchain can meet the needs of IoT devices for network access in the case of movement. In addition, the high security of blockchain data storage provides a good guarantee for data sharing and collaborative work after IoT devices are accessed (TAN Chen. 2020). Several IoT platforms, such as IOTA, IBM Watson IoT, VeChain, and Ambrosus, are incorporating blockchain technology for identity management to enhance security and transparency. IOTA ensures secure device communication through decentralized authentication mechanisms, and IBM Watson IoT utilizes blockchain to record device identities for a transparent and tamper-proof ledger. VeChain focuses on supply chain management, tracking device history to ensure authenticity, while Ambrosus monitors the food and pharmaceutical supply chain via blockchain, verifying sensor identities and enhancing data reliability and consumer trust. These platforms take advantage of blockchain to significantly improve the security and transparency of IoT devices.

B. Design of access control mechanism

The access control mechanism makes full use of the blockchain's characteristics of decentralization, transparency and non-tampering to achieve transparency, traceability and traceability of the access process under the premise of protecting the privacy of the object resources (Hui, L. I., &

Guozhen, S. H. I. 2020). The access control policy is deployed on the blockchain in the form of a smart contract. This makes the whole access authorization process transparent, and the access control decisions are realized by executing the smart contracts deployed on the blockchain. In order to protect the privacy of client resources, a combination of off-chain and on-chain approaches is used. The guest resources are stored in the semi-trusted data server under the chain, and the guest index is generated and stored on the guest blockchain through the guest storage address, summary, and other information. The authorized subject accesses the object resources through the object address. For the authorized subject to send access credentials, the access credentials are deployed on the blockchain. The access credentials carry access rights and conditions to be met, and when the subject accesses the object, the blockchain verifies the authenticity and trustworthiness of the access credentials to realize fine-grained access control. The log blockchain records access authorization logs and access logs, and the log blockchain achieves traceability and traceability of access authorization and access process. At the same time, it adopts the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to record the process of intelligent access control policy deployment, object deployment, access authorization, access authorization logging, access logging, and other processes into the blockchain.

The access control mechanism is realized by the role security management server, which on the one hand assigns roles and manages roles; on the other hand, it acts as an authentication server to issue role certificates for users. The main modules of the role security management server are the authentication module, role management module, key management module, certificate management module, user interface module, and network communication module. When a user makes an authentication request to the role security management server (including user name, password, and applied role), the identity verification module of the role security management server verifies the user's identity. After verification, the user/role management module queries the user and role database according to the user's identity, assigns the corresponding role to the user, and generates a role certificate together with the role key generated by the role key management module and sends it to the user together. DSAS has an access control decision-making module on the storage server, which sets up checkpoints before the access operation and determines whether to accept the access request or not by using the role/permission database. The DSAS has an access control decision module on the storage server. After receiving an access request, the storage server queries the role/permission database to determine whether the user can access resources using the file access interface provided by GlusterFS according to the user's role authorization. The role management module calls the information in the role access information database, and the control decision module determines the access rights of the subject. The role information database stores access subject information, access object information, and access control role information.

V. Conclusion and Future Work

This study emphasizes the importance of authentication and access control in IoT security and describes the limitations of existing mechanisms. With the proliferation of IoT devices, traditional authentication and access control methods may not be able to meet the increasingly complex security requirements. The shortcomings of these mechanisms in terms of adaptability, flexibility, and real-time performance may lead to potential security risks. Therefore, to address these issues, future research can focus on the following directions:(1) Exploring the application of blockchain technology: blockchain technology shows great potential in identity management, especially in terms of decentralization, security, and transparency. However, how to effectively address technical barriers in blockchain implementation (e.g., scalability, performance, and privacy issues) is still a topic that deserves in-depth research. Future work could focus on exploring how to combine blockchain with existing identity management systems to enhance security in IoT environments. (2) Enhance user experience: research on how to enhance security while also optimizing user experience to reduce user resistance to using authentication and access control mechanisms that are too cumbersome. Adopting a simplified authentication process and multiple verification methods can effectively improve user acceptance and satisfaction. (3) Dynamic access control policies: future research should focus on developing and optimizing dynamic access control policies that can be adjusted in real time based on contextual information (e.g., user's location, time, and device type) to cope with changing security requirements.

In summary, with the continuous development of IoT technology, there are still many pending challenges in the field of authentication and access control. By introducing advanced technologies and methods, more comprehensive and effective solutions can be provided for IoT security.

References

1. Zang Jingsong. (2010). *Safety Performance AnaIysis on Internet of Things*, 6, 51-55.
2. TAN Chen. (2020). *Research on distributed identity authentication mechanism of IoT device based on blockchain*. Chinese Journal on Internet of Things[J], 4(2), 70-77.
3. Guo, Y., Guo, Y., Xiong, P., Yang, F., & Zhang, C. (2024). *Deeper insight into why authentication schemes in IoT environments fail to achieve the desired security*. IEEE Transactions on Information Forensics and Security.
4. Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). *Multi-factor authentication: A survey*. Cryptography, 2(1), 1.
5. Kaur, A. A., & Mustafa, K. K. (2019). *A Critical appraisal on Password based Authentication*. International Journal of Computer Network and Information Security, 11(1), 47.
6. Hui, L. I., & Guozhen, S. H. I. (2020). *Blockchain-based access control mechanism for data traceability*. Journal on Communications, 41(12), 82-93.
7. Shay, R., Carone, M., & Miller, R. (2016). The effectiveness of phishing training: A study of user

behavior. Computers & Security, 62, 19-28.
8. Ratha, N. K., Bolle, R. M., & Connell, J. H. (2018). Biometric Authentication: A Review. IEEE Transactions on Information Forensics and Security, 3(2), 207-221.