# Blockchain-Based Privacy Protection for IOT Devices in Smart Communities

Tuli Chen[1], Fu Luo[1], Wennan Wang[1], Shiyang Song[2, *], Chengyifan Li[2], Yi Dong[3]

chentuli10@126.com, luofu13971624561@163.com, wwwennan@163.com, *Corresponding author E-mail: 2463756962@qq.com, lllchengyf02@163.com, xcldongyi@163.com

[1]School of management, Guangdong University of science and technology, Dongguan, China

[2]Alibaba Cloud Big Data Application College, Zhuhai College of Science and Technology, Zhuhai, China

[3]Xinchang Road Primary School, Zaozhuang, China

**Abstract:** Thanks to the spread of IOT technology, IOT is becoming more and more common in business and people's daily life. Smart buildings are a huge area of IOT research and application. Modern cities cannot be built without the benefits brought by IOT, including speed, security and low cost. This paper focuses on security and privacy issues in IOT, especially in the area of smart communities (community access control systems), where the massive collection and excessive misuse of personal data has created many new needs that must be addressed by the development of smart communities. In these environments, there is a need not only for secure and applicable engineering solutions to protect privacy, but also for large-scale implementation of policies. This is to ensure that any sensitive information that needs to be handled is handled appropriately. This paper proposes an improved Cartographic Block-chain (CBC) block-chain technology based on Advanced Encryption Standard (AES) that contributes to the management of personal data collection and information access in smart buildings. The technology shared keys will be assigned to communication devices connected to smart access control, enhancing the control of sensitive private data in smart communities. Blockchain's technology can provide stronger security services for IOT applications.

**Keywords:** privacy protection, blockchain technology, information safety.

## 1. Introduction

The Internet of Things has been called humanity's "fourth industrial revolution" and modern information and communication technologies are playing a key role in the daily lives of governments, organizations and billions of people around the world. The tremendous capabilities brought by the development of IOT technologies bring convenience and risk to almost all industries, as most aspects of an individual's life depend on technology. How modern services "intrude" into the private lives of individuals and how to protect their private information is a question worth pondering, both from a technical and legal perspective. Current security and privacy issues, as well as the policies used by organizations, businesses, public administrations, oversight bodies and authorities to collect and manage personal data, are major issues in the development and maintenance of the Internet of Things today and in the future.

BDEIM 2022, December 02-03, Zhengzhou, People's Republic of China

DOI 10.4108/eai.2-12-2022.2328716

Privacy information leakage as a hot issue in today's academic research, the study of privacy leakage of smart community occupants should be given sufficient attention. The research on privacy leakage of smart community occupants is not only helpful to enhance the understanding of privacy information leakage problem in academic circles, but also can provide strong support to the healthy development of smart communities in the new era. Blockchain computing can be used as part of a security framework to protect many IOT-oriented applications, as it ensures integrity and privacy even when datasets are released to the public [1].

### 1.1 Internet of Things

The Internet of Things (IoT), the "Internet of Everything", is a huge network of interconnected sensor devices connected by the Internet. In this network, various devices in the Internet of Things can exchange information and communicate to achieve intelligent management and control of various devices. 2005, the International Telecommunication Union officially proposed the concept of "Internet of Things" in the "ITU Internet Report 2005: Internet of Things", in which radio frequency identification technology (RFID), sensor technology and wireless communication technology were added to the Internet of Things. In 2005, the International Telecommunication Union officially proposed the concept of "Internet of Things" in the "ITU Internet Report 2005: Internet of Things", which added RFID, sensor technology and wireless communication technology to the Internet of Things, making the Internet of Things begin to be applied in various fields, marking the advent of the "Internet of Things Era" [2] Although the Internet of Things brings us a IOT of convenience, it also brings us a IOT of privacy leakage problems. Users may face the problem of privacy leakage in requesting data, transmitting data, storing data and sharing data. The leakage of users' privacy information may not only cause users' economic loss, but even endanger their lives [3].

Therefore, while using IOT to bring convenience to people, we should pay more attention to the security and privacy leakage problems in IOT, and we need to ensure the security, reliability and confidentiality of data in all aspects of data request, transmission, storage and sharing to prevent unscrupulous elements from violating users' privacy through IOT devices and systems. In addition, IOT terminal devices usually have weak computing power and limited transmission capability, and IOT systems and devices of different application scenarios often have their own characteristics. At the same time, different kinds of IOT applications have different requirements for data collection, transmission, storage and sharing. Some IOT applications need to focus on data loss and access control issues, some need to focus on the computational consumption and fragility of sensor devices, some need to focus on trusted data collection, high real-time transmission and human factors, and some need to focus on

Others need to focus on data traceability, tamper-evident storage, and multi-party data sharing.

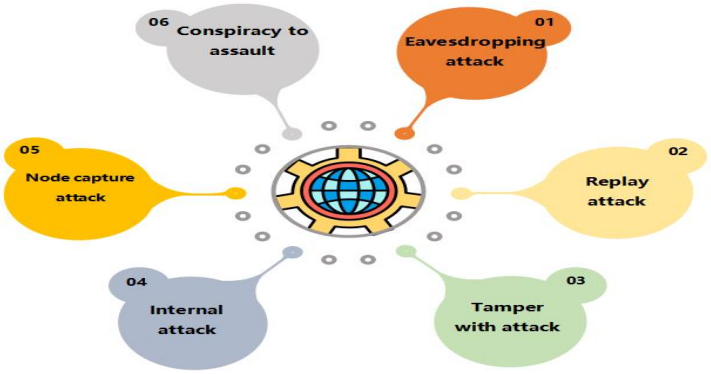


Figure1. Threat model for securing internet of things (IOT)

### 1.2 Blockchain

Blockchain technology, introduced with Bitcoin, is a revolutionary application model that incorporates various computer technologies such as cryptographic algorithms, consensus mechanisms, distributed data storage and peer-to-peer transmission. Essentially, a blockchain is a network of computer systems that replicates and distributes a digital ledger of transactions. Blockchain blocks contain many transactions, and every time a new transaction occurs, it is recorded in the ledger of each participant. Distributed ledger technology [4] enables multiple nodes to maintain a decentralized database, reducing both security and cost problems. The blockchain contains many blocks, which are stored after consensus is reached. When smart contracts are implemented, blockchain technology can make the IOT more secure. A smart contract is a computer program or script that has a unique address on a blockchain network. Peer-to-peer messaging is much faster and easier to manage with peer-to-peer networking than with centralized systems due to the elimination of a central server. It also enhances fault tolerance and scalability. Using smart contracts, IOT systems can be made more secure.

### 1.3 Smart Community

In the IOT world, the demand for data encryption solutions is growing, and the leakage of smart community residents' privacy will bring huge risks, such as the loss of personal information and theft by others, resulting in personal and economic losses to the residents. In serious cases, the property management system will be paralyzed and unable to operate normally, leading to the deterioration of the development of smart communities and adverse development. Therefore, the study of the risk of privacy leakage of the residents of the smart community is conducive to the prevention of the above problems that may bring about the risk of the ground, the confidentiality of the residents' own privacy, the protection of the economic property of the residents from the aspect of privacy, the promotion of the change and improvement of the property management of the smart community, and the promotion of the continuous improvement of the smart community as a whole.

In the design of the access control system in the smart community, it is mainly composed of the system service terminal, access control management service terminal, electronic lock, etc., of which the electronic lock is the core part, consisting of door lock, identity reader, access control, network camera, buzzer and backup power supply. The access controller mainly real-

izes ID card information reading, face recognition, alarm processing and door opening processing.

## 2. Blockchain in the Internet of Things

Transmitting data over a network connection requires data encryption. Information confidentiality, secrecy and validity can be assured through the use of cryptographic systems. The CP-ABE scheme uses ECC in its key management system. Unlike other schemes, this scheme requires the recipient's private key to decrypt the message if a semi-trusted authority produces a key [7]. To protect the security of IOT devices, communication should be encrypted. However, because IOT device components have limited resources, such as battery power, processing power, and storage capacity, developing solutions based on traditional encryption methods is a daunting task. IOT devices, however, require a IOT of processing power and are not compatible with traditional encryption techniques. In resource-limited IOT environments, some devices require a much less expensive security solution. Although edge devices may be able to handle standard cryptographic languages, their fast battery life, low computational power consumption, small size, insufficient power, and short battery life limit their use of cryptography.

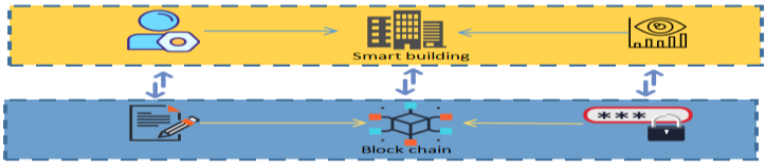


Figure 2 Block chain in smart building

## 3. Blockchain Encryption Algorithm

Key exchange paradigms should be considered in IOT applications since data security is critical. We use asymmetric encryption with AES-CBC for encrypting data in this study. With its short execution time, this encryption is suitable for smart tasks with limited processing resources that require high speed. An agreed-upon key is known by both parties.

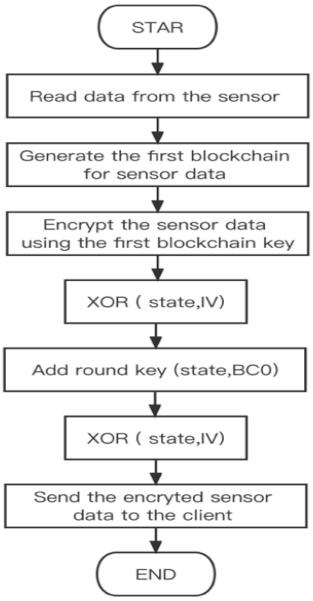


Figure 3 Encryption algorithm

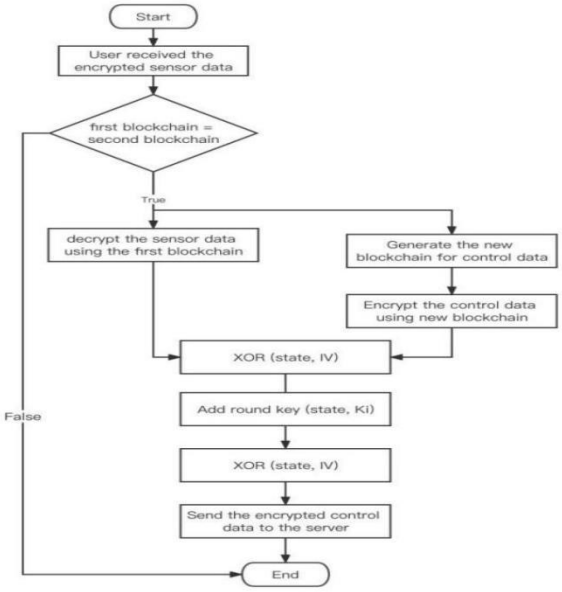


Figure 4 Decryption algorith

## 4. Analysis of results

It has been demonstrated that improved AES-CBC symmetric encryption and blockchain technology can ensure the confidentiality, integrity, and availability of security services. When evaluating a method, it is imperative to consider the time taken to execute the algorithm in an IOT environment and the creation of a shared key. In addition to providing a high level of security, the method must be fast and efficient. Comparing the improved AES-CBC algorithm with the classic AES-CBC algorithm is the purpose of this study. Encrypting and decrypting the specific data received from the sensor requires a calculated amount of time. With the blockchain algorithm, 100-byte files are stored on the blockchain enabling much faster execution times than with AES-CBC without blockchain. Compared to the original AES-CBC algorithm, the improved algorithm uses blockchain technology. Thus, the method considered is well suited to protecting information in smart buildings.

It is imperative to evaluate any algorithm used in an IOT environment based on its execution time; therefore, Table 2 shows the average encryption time for different numbers of users (1-100) based on the improved AES-CBC encryption algorithm based on blockchain technology. For each control command that modifies the device state, it is necessary to increase the time required for the encryption and decryption of the data received from the sensors. The number of users connected to the IOT directly determines how long it will take the server to decode the set message size. Various statistical techniques can be used to evaluate cryptographic algorithms' randomness. The paper uses 50 data sets to examine the proposed method. It also shows statistical tests show it is effective and passes all statistical randomness tests after running both algorithms on a text file for a certain period of time.

Table 1. Execution time

| Algorithm | Average encryption time |
|---|---|
| AES–CBC | 0.1656 |
| Modified ARS–CBC | 0.0666 |

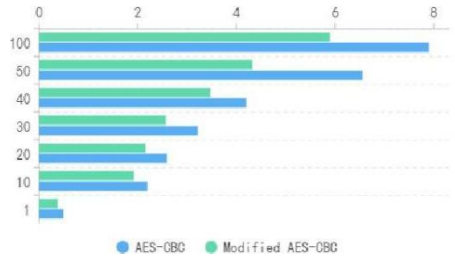


Figure 6 The average execution times

## 5. Conclusion

Physical objects are more easily integrated into the digital world thanks to ubiquitous computing. IOT has become an integral part of business and daily life over the last decade. IOT's ability to provide security and cost effectiveness is crucial to the use of ICT in e-health. Authentication between different users of a unified smart home resource is performed using smart contracts and blockchain technology. A major benefit of this development is the ability to access information in a smart building with increased efficiency and security. This is because other third parties will need to authenticate each time they access information. Based on the results, it can be demonstrated that AES-CBC-based blockchain technology is effective in providing secure services to IOT applications and ensuring a short execution time.

## References

[1] Y. Yuan and F. -Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421-1428, Sept. 2018, doi: 10.1109/TSMC.2018.2854904.

[2] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80, 1-50.

[3] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta and A. Bhatnagar, "CRAIoT: Concept, Review and Application(s) of IoT," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777467.

[4] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151.

[5] Y. Jiang et al., "Secure Data Transmission and Trustworthiness Judgement Approaches Against Cyber-Physical Attacks in an Integrated Data-Driven Framework," in IEEE Transactions on

Systems, Man, and Cybernetics: Systems, vol. 52, no. 12, pp. 7799-7809, Dec. 2022, doi: 10.1109/TSMC.2022.3164024.
[6] Sadeeq, M. A., Zeebaree, S. R., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018, October). Internet of Things security: a survey. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 162-166). IEEE.
[7] Sowjanya, K., Dasgupta, M., & Ray, S. (2021). A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IOT healthcare systems. Journal of Systems Architecture, 117, 102108.