IoT Data Privacy Protection Scheme based on Blockchain

Yue Wu\textsuperscript{1,2,*}, Liangtu Song\textsuperscript{1,2}, Lei Liu\textsuperscript{1,2} and Qijin Wang\textsuperscript{1,2}

\textsuperscript{1}Institute of Intelligent Machines, and Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, Anhui, PR China
\textsuperscript{2}University of Science and Technology of China, Hefei 230026, Anhui, PR China

*Corresponding author: wuyue@iim.ac.cn

Abstract. This article introduces the blockchain technology and proposes a blockchain-based IoT sensor data privacy protection scheme from the anonymisation of user identity, the protection of private data and the procedure that allows third parties to use encrypted sensor data. The sensor and the gateway establish a connection after authentication and key negotiation, and the sensor periodically uploads the sampled data and hash-based message authentication code (HMAC) to the gateway. After the gateway verifies the HMAC code of the sensor data, it encrypts the sensor data, constructs a blockchain transaction and submits it to the blockchain node. Blockchain nodes cache transactions and periodically generate blocks to confirm that the transactions are on the chain. After the gateway constructs an authorised transaction and submits it to the blockchain node for confirmation, the designated decentralised application (DApp) obtains the permission and related keys to access the designated sensor managed by the gateway. Finally, the DApp queries the local blockchain node for the specified sensor data and decrypts the results. Experiments have proven through in-depth discussions on sensor synthesis data, sensor/gateway verification, transaction data encryption and transaction signatures that the scheme can be used in IoT systems.

1. Introduction

With the continuous development and advancement of sensor technology, computer control technology, embedded technology and wireless network data communication technology, the Internet of Things (IoT) has shown tremendous development worldwide [1]. The IoT is considered to be the wave of the third world information industry after computers and the Internet and is developing rapidly. By 2020, more than 50 billion smart devices will be connected to the network [2]. Distributed processors and communication hardware send/receive data from the environment, thereby generating large amounts of data [3]. However, most IoT architectures currently require a central hub or server to allow data storage and transmission between multiple devices in cyberspace [4]. These smart devices use sensors, embedded processors and communication hardware to send/receive data from the environment, thereby generating large amounts of data. Therefore, security and privacy have become the biggest challenges of the IoT [5] [6].

This article mainly studies how to solve the problem of active privacy protection of the sensor data of the IoT based on the blockchain, such as the privacy protection of the family or personal sensor data in the smart grid and smart medical care [7]. The first major privacy issue is the issue of user identification on the blockchain IoT, that is, the issue of anonymisation. Although blockchain generally
uses asymmetric key pairs to identify user identities and does not require centralised registration, users have a certain degree of anonymity, but tracking the transaction information of the user’s identity and associating it with other information are possible [8][9]. Found many clues can be found about the true identity of anonymous users. Blockchain data analysis has become a big business. The government uses it to investigate suspicious crimes, and digital currency exchanges use it to track the compliance of customers’ funding sources. Thus, this study first investigates the anonymisation of user identities on the block IoT [10] [11]. Although the blockchain cannot be tampered with, the data on the blockchain is open and transparent and can be viewed by everyone. Thus, this article also considers the protection of private data on the blockchain IoT [12]. Although encryption is an indispensable solution for protecting private data considering the possibility that IoT data may be used by third parties after they are on the chain, a pure encryption solution is not enough. For example, power companies need to use household energy consumption data to generate bills, and doctors need to use patients’ wearable device test data for diagnosis and treatment [13]. Thus, this article determines how to let third parties use encrypted sensor data.

2. System Model

2.1. Sensor data flow

In the solution proposed in this study, the entire sequence of data from the sensor to the gateway used by the third party is shown in Figure 1.
The sensor and the gateway establish a connection after authentication and key agreement. The sensor regularly uploads sampled data and hash-based message authentication code (HMAC) to the gateway. After the gateway verifies the HMAC code of the sensor data, it encrypts the sensor data, constructs a blockchain transaction and submits it to the blockchain node. Blockchain nodes cache transactions and periodically generate blocks to confirm transactions on the chain. After the gateway constructs an authorised transaction and submits it to the blockchain node for confirmation, the designated DApp obtains the right to access the designated sensor managed by the gateway and related keys. DApp queries the local blockchain node for the specified sensor data and decrypts the results.

2.2. Privacy protection mechanism
This article mainly uses the following mechanisms to realise the privacy protection of IoT sensor data based on blockchain:

Gateway identity authentication mechanism: The ECDH algorithm-based identity authentication mechanism is used between the sensor and the gateway to realise the identity authentication of the sensor to the gateway and avoid access to the gateway forged by the attacker.

Sensor data verification mechanism: Sensor data uses HMAC to ensure data source and integrity.

Gateway transaction data encryption mechanism: After the gateway verifies the sensor data, it uses the gateway’s ECC public key encryption algorithm to generate blockchain transactions on the chain to ensure that private data is not leaked.

Gateway transaction source anonymisation mechanism: Only blockchain transactions generated by the gateway use Borromean ring signature algorithm to anonymise the transaction source.

On-chain data access control mechanism: The sensor data on the chain is protected by an attribute-based access control (ABAC) mechanism.

Third-party utilisation mechanism of encrypted data: Only the encrypted sensor data on the chain can be decrypted by a third party authorised by the proxy re-encryption (PRE) algorithm.

3. Experimental evaluation
Transaction delay time is an important indicator to measure system performance. It represents the time from transaction submission to block confirmation. From the sensor sending data to the final transaction entering the block, the total delay time can be divided into two segments.

\[ \text{Latency} = L_1 + L_2 \]  

(1)

\( L_1 \) represents the time when the sensor is submitted to the gateway to complete the detection, and \( L_2 \) represents the time from when the gateway submits the transaction to when it is packaged into the block. In this part, we experiment with different parameters of the system and analyse the influence of these parameters on system performance.

Sensor-gateway verification: disable and enable
Transaction signature: no signature/ECC signature/ring signature
Sensor data encryption: no encryption/ECC public key encryption

The experiment is based on the Python simulation environment, and the system topology is shown in Figure 2.
Figure 2. System configuration.

We use sensor–gateway verification and no-verification schemes to investigate the impact of this link on performance. The experimental parameters are as follows:

- Blockchain node generation cycle: 5000 ms
- Sensor data upload cycle: 1000 ms
- Sensor data synthesis: enable
- Sensor-gateway verification: enable/disabled
- Easy data encryption: disabled
- Transaction signature format: no signature

The following figure shows the statistical histogram of $L_1$ time under two different scenarios (Figures 3 and 4).

Figure 3. No sensor/gateway verification.
The above figures show that enabling and not enabling sensor/gateway encryption has no obvious impact on the L1 delay time. The difference between the two is mainly the use of different sensor data integrity verification mechanisms. When sensor-gateway verification is not enabled, SHA256 is used. HMAC is used when sensor-gateway authentication is enabled. The result of the above figure shows that the computational efficiency of HMAC in the simulation system is slightly higher than that of SHA256.

4. Conclusion
This study proposes a data privacy protection scheme for IoT sensors based on blockchain. The sensor and the gateway establish a connection after authentication and key negotiation, and the sensor periodically uploads the sampled data and HMAC to the gateway. After the gateway verifies the HMAC code of the sensor data, it encrypts the sensor data, constructs a blockchain transaction and submits it to a blockchain node. Blockchain nodes cache transactions and periodically generate blocks to confirm that the transactions are on the chain. After the gateway constructs an authorised transaction and submits it to the blockchain node for confirmation, the designated DApp obtains the permission and related keys to access the designated sensor managed by the gateway. Finally, DApp queries the local blockchain node for the specified sensor data and decrypts the results. In the plan, through in-depth discussions on sensor synthesis data, sensor/gateway verification, transaction data encryption and transaction signatures, experiments have shown that the performance of the system meets actual needs, and the program can be applied to IoT systems.

Acknowledgments
This study was supported by Key Research and Development Plan of Anhui Province (201904a06020056).

References
[1] Yue Wu, Liangtu Song, Lei Liu, Jincheng Li, Xuefei Li, Linli Zhou, "Consensus Mechanism of IoT Based on Blockchain Technology", Shock and Vibration, vol. 2020, Article ID 8846429, 9 pages, 2020. https://doi.org/10.1155/2020/8846429.
[2] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges,"
[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[4] S. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of IoT infrastructure with Ethereum transactions," Iran Journal of Computer Science, vol. 2, no. 3, pp. 189-195, 2019.

[5] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and privacy," arXiv preprint arXiv:1712.02969, 2017.

[6] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications policy, vol. 41, no. 10, pp. 1027-1038, 2017.

[7] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481-2501, 2014.

[8] A. Kiayias and G. Panagiotakos, "Speed-Security Tradeoffs in Blockchain Protocols," IACR Cryptology ePrint Archive, vol. 2015, p. 1019, 2015.

[9] D. Guinard, V. Trifa, and E. Wilde, "A resource oriented architecture for the web of things," in 2010 Internet of Things (IOT), 2010: IEEE, pp. 1-8.

[10] Q. He, N. Guan, M. Lv, and W. Yi, "On the consensus mechanisms of blockchain/dlt for internet of things," in 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), 2018: IEEE, pp. 1-10.

[11] Krishnan, M.A.; Shankar, C.G.; Raj, S.A.; Ragavan, A. Peer to Peer File Sharing by Blockchain Using IOT.2017. Available online: http://ijsrset.com/IJSRSET173253 (accessed on 30 April 2017).

[12] Wu, L.; Du, X.; Wang, W.; Lin, B. An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC 2018), Maui, HI, USA, 5–8 March 2018.

[13] Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017; pp. 464–467.