Journal of Organizational and End User Computing
Volume 35 • Issue 3

Application of Internet of Things and Blockchain in Information Security and Privacy Protection of Global Organizations

Shuya Fang, Zhoukou Normal University, China

Qingquan Liu, Jiaxing University, China

Fengrui Zhang, Sichuan Agricultural University, China

Ningyan Chen, University of Aberdeen, UK

Xin Li, Jiaxing University, China*

ABSTRACT

Access control data will continue to be exposed to the threat of privacy leakage even if blockchain technology currently offers a new solution for the security and privacy of the internet of things (IoT). However, its usability and privacy are not completely leveraged. This paper first discusses the IoT and blockchain technology and then examines each technology's structural models in order to address the issue of information security and privacy protection for the global organization IoT based on blockchain. Second, the information security and privacy guarantee system based on blockchain is built with ZKP and TEE at its heart after problems with zero-knowledge proof (ZKP) and trusted execution environment (TEE) in information security guarantee based on blockchain are investigated. By comparing the simulation trials, the proposed system's viability is finally confirmed. The results demonstrate that the suggested algorithm's evidence generation time is 352 ms when it reaches the experiment's highest node 28, which is clearly faster than previous techniques.

KEYWORDS

Blockchain, Information Security, Internet of Things, Privacy Protection, Trusted Execution Environment, Zero Knowledge Proof

INTRODUCTION

The Internet of Things (IoT) has increased worldwide thanks to the development of smart gadgets and the fifth-generation mobile communication network. It has so far been utilized in the fields of transportation, intelligent manufacturing, health care, finance, petrochemical and other businesses, and urban infrastructure, and it is having an ever-growing impact on the market (Li et al., 2021). The

DOI: 10.4018/JOEUC.323192

*Corresponding Author

scale of management devices may come from millions to hundreds of organizations, enterprises, or institutions due to the widespread dissemination of IoT devices. Using the traditional method of user name and password to log in to the system is a huge amount of work and a significant risk of password leakage (Khando et al., 2021). In the IoT, access control is a security mechanism to prevent the leakage of resources, which is used to grant or cancel access rights to specific users for the specified IoT resources. The traditional centralized access control system is suitable for human-machine oriented internet scenes, the devices are in the same trust domain, which cannot meet the access control requirements of the IoT, and the traditional access control model has problems such as single point of failure (Mohammed, 2021). Aiming at this problem, blockchain technology provides a new solution for access control and security protection of the IoT. Blockchain presents a decentralized architecture for the IoT through peer-to-peer networks. Data can no longer be managed and controlled by large centralized servers. A large amount of data in the IoT will be encrypted before transmission so that users' information and privacy will be more secure.

Academics have conducted many studies on the IoT's information security and privacy protection. Ferrag et al. proposed a security and protection system for basic federated learning, one type of IoT technology, and also discussed new technologies like blockchain and malware/attack using essential federated learning as basic IoT technology. They also proposed three deep learning technologies, including a recursive neural network (RNN), a convolutional neural network (CNN), and deep neural network (DNN) with a recursive architecture. Experimental analysis of the collaborative deep learning approach for network security in IoT applications reveals that it is more effective than traditional/centralized machine learning in protecting the privacy of IoT device data and at detecting assaults (Ferrag et al., 2021). The study uses deep learning technology to ensure the privacy of the data of IoT devices. Ferrag and Shu summarized the existing investigations on the security of the IoT network blockchain, reviewed the security and privacy systems of four IoT applications based on blockchain, compared nine attributes of various consensus algorithms, including delay, throughput, calculation, storage and communication costs, scalability, attack model, advantages and disadvantages, etc. They also analyzed the performance indicators, blockchain test platform and cryptography library used in the performance evaluation of the IoT network security and privacy system based on blockchain.

Finally, the open challenges and future research opportunities were discussed (Ferrag, & Shu, 2021). The research is a summary of the current blockchain IoT network security and privacy system, which provides people with the idea of using blockchain technology to protect the information security of the IoT. The IoT system's security and privacy concerns were highlighted as Deep et al. studied the security issues of each layer in the IoT protocol stack, identified the potential difficulties and essential security requirements, and briefly described the current security solutions to protect the IoT from the layered environment (Deep et al., 2022). The research aims at the security problems of all layers of the IoT protocol stack, and protects the security and privacy of the IoT in layers. Zeadally et al. focused on introducing the encryption protocol standards that were currently being used or advised for IoT devices to ensure secure communication, as well as the benefits and drawbacks of several protocol standards that were suitable for different IoT application scenarios (connected cars, health, smart homes and consumer appliances and devices). The final topic covered various issues with encryption protocol standards that need to be resolved for IoT applications (Zeadally et al., 2021). The object of this study is the encryption protocol for secure communication of IoT devices to ensure the communication security of IoT. To ensure the safety of IoT devices for tracking and treating pandemic diseases, Shu et al. divided existing security systems and privacy schemes into five categories: identity authentication system and access control scheme, essential control and password scheme, blockchain-passing scheme, intrusion system, and protection scheme. For each category, they also identified relevant challenges and recommendations (Shu et al., 2021). They put forward suitable protection suggestions for the IoT devices that monitor and treat epidemic diseases. To address the network security challenge, Djenna et al. critically examined current network security issues of key IoT-based infrastructure, discussed potential network threats, network vulnerabilities, and the primary utilization strategies used by cybercriminals, provided the classification of network attacks that may affect key network infrastructure, and proposed security requirements as well as some practical suggestions to improve network sec (Djenna et al., 2021). The research ensured the network security of the IoT infrastructure. In short, the above research or deep learning is combined to study the security and privacy system of IoT applications, or analyze the current encryption protocol standards used for IoT devices to ensure secure communication, or provide solutions to the security problems of each layer in the IoT protocol stack, or to put forward security requirements and suggestions from the critical infrastructure of the IoT. Still, none of them is combined with blockchain to study global organisations' information security and privacy protection.

Based on the above background, this paper starts with the technical models of IoT and blockchain technology, analyzes the ZKP and TEE technology used to protect information and privacy in blockchain, innovatively combines them, and proposes an IoT information security and privacy protection system based on blockchain technology based on ZKP-TEE fusion algorithm. Finally, the performance of the proposed fusion algorithm is verified by simulation experiments and comparative experiments with the proof generation time and verification time of the proof algorithm as indicators. The study on the worldwide organization's approach to protecting privacy and information security blockchain technology applied to IoT can offer a theoretical foundation for the security of information and privacy and some practical implications for information leakage.

METHOD

Overview of IoT and Blockchain Technology

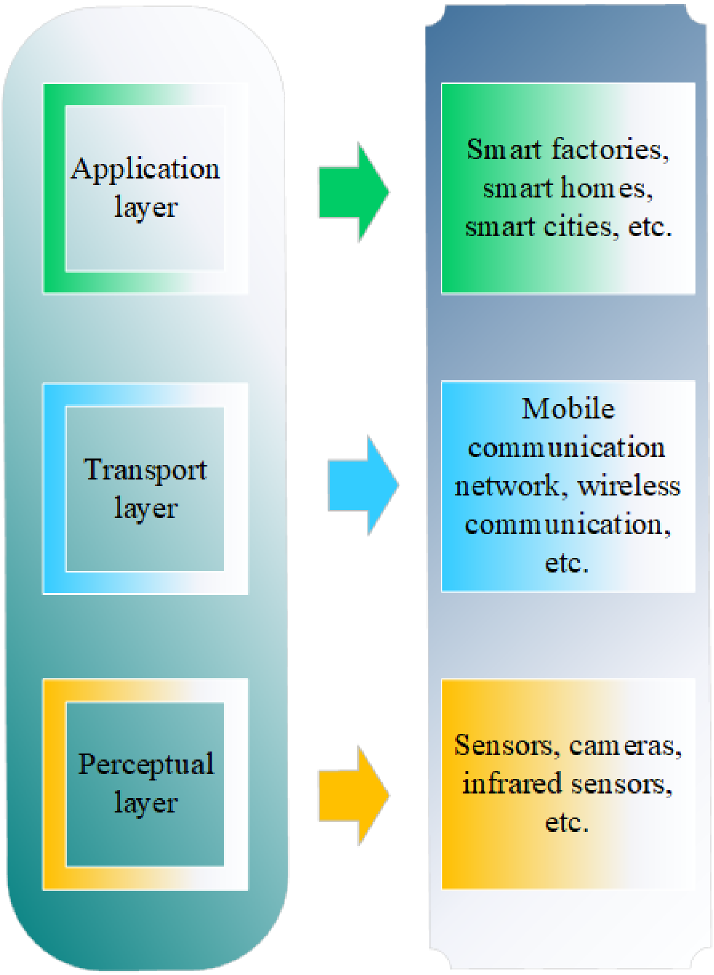
The IoT is a network that enables any object or device to communicate with the internet through a predefined protocol to realize a more innovative world (Nguyen et al., 2021). Figure 1 depicts the overall IoT architecture.

Figure 1 illustrates how the IoT can be separated into three layers: perceptual, transport, and application (Choi et al., 2021; Koohang et al., 2022). As an essential foundation for building the IoT, the perceptual layer is the main data source of the whole network. The transport layer collects information from the perceptual layer and provides a safe, stable and effective information exchange platform between the perceptual and application layers. The application layer is responsible for processing the data of the perceptual layer and managing and maintaining it, which is the crucial point to realize the specific functions of the IoT. The scarcity of technological IoT security protection tools and frequent IoT information system security incidents have drawn significant attention from nations worldwide. Researchers in the field of IoT security are interested in the underlying blockchain technology that the emergence of Bitcoin has brought forth.

The public critical cryptography method, hash algorithm, consensus management mechanism, and other advanced technologies are all included in blockchain's highly decentralized distributed database information technology. It synthesises certain established or emerging information technologies that establish a secure and reliable working environment for the blockchain network system while utilizing diverse information technologies effectively (Ali et al., 2021; Javaid et al., 2021). Figure 2 illustrates the six levels that make up the blockchain technology model: application layer, contract layer, excitation layer, consensus layer, network layer, and data layer.

The consensus layer, the network layer and the data layer in Figure 2 are the three essential core layers of the blockchain network. The term "consensus layer" describes the consensus formula utilized in many blockchain networks. Following the "longest chain concept," consensus calculation is primarily employed to guarantee the consistency of shared data information across nodes throughout the whole network. Without trusted third-party services, the network layer is used to complete point-to-point connections and interactions between nodes. The data layer mainly includes the information formed by stock trading in the whole network, including trading data information, one-way chain

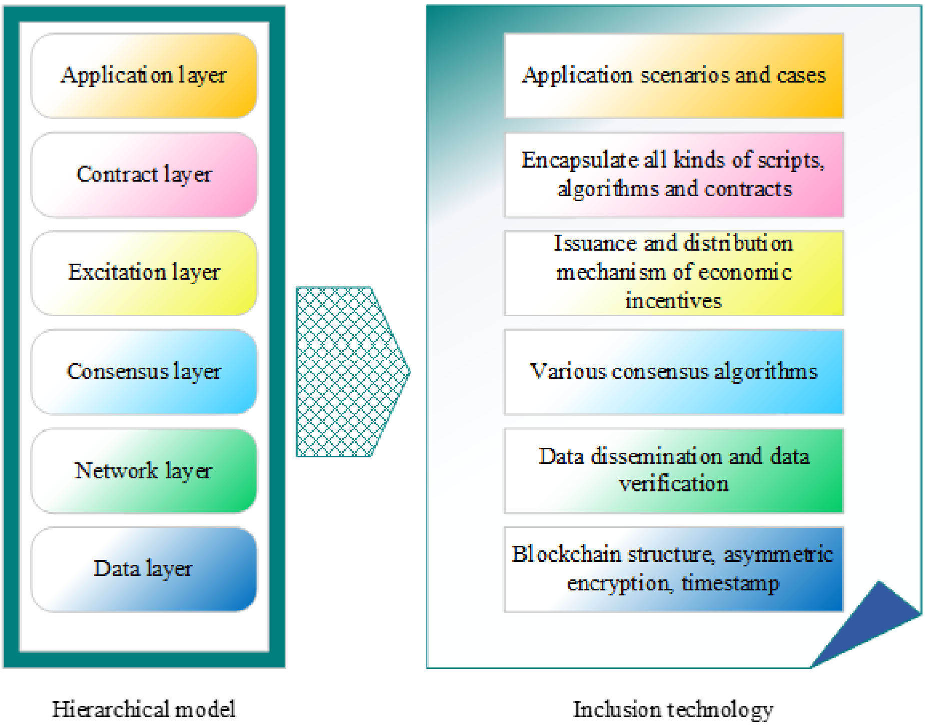
Figure 1. General overall architecture of the IoT


Application layer
Smart factories, smart homes, smart cities, etc.
Transport layer
Mobile communication network, wireless communication, etc.
Perceptual layer
Sensors, cameras, infrared sensors, etc.

structure, random number and customer public key (Alsharari, 2021; Lim et al., 2021; Sekar et al., 2022).

Blockchain technology is widely employed in all spheres of life and has advanced significantly because of its benefits of decentralization, tamper resistance, high traceability, transparency, and privacy (Garg et al., 2021). The application of blockchain technology to the IoT's information security and privacy protection is embodied in the IoT's access control and privacy protection (Egala et al., 2021; Liu et al., 2021). Access control schemes are divided into two categories: access control based on bitcoin and access control based on smart contract, such as using new types of transactions to grant, obtain, delegate or cancel access rights. The decentralized electronic medical management record system using blockchain technology uses three kinds of intelligent contracts: registration contract, doctor-patient relationship contract and authorization contract for electronic medical record access control. In terms of privacy protection, Microsoft proposed a framework to protect blockchain privacy using TEE. This secret alliance framework includes a set of secret keys and authority management mechanisms, ensuring that only encrypted transactions can be loaded into the TEE for execution, and only users with corresponding rights can view the relevant status.

Figure 2. Blockchain technology model


Application layer
Contract layer
Excitation layer
Consensus layer
Network layer
Data layer
Application scenarios and cases
Encapsulate all kinds of scripts, algorithms and contracts
Issuance and distribution mechanism of economic incentives
Various consensus algorithms
Data dissemination and data verification
Blockchain structure, asymmetric encryption, timestamp
Hierarchical model
Inclusion technology

Analysis of Zero-Knowledge Proof and Trusted Execution Environment

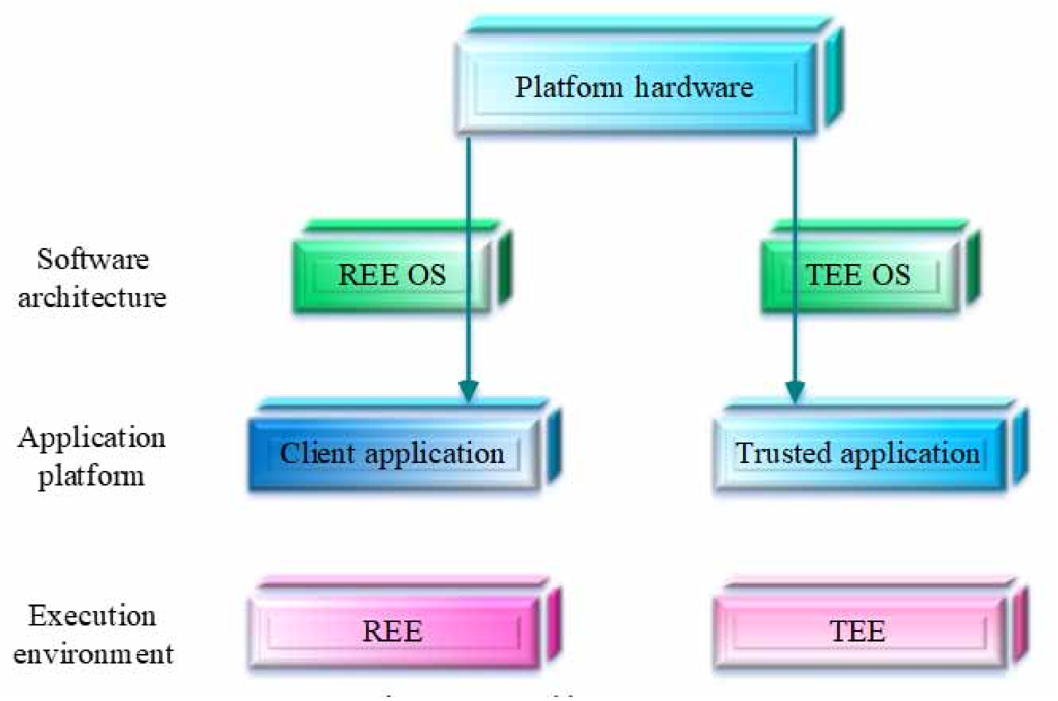
ZKP is a type of promise-based proving technique. For the verifier to feel certain that the prover knows the secret and is telling the truth, the prover must demonstrate his knowledge of the secret while refusing to divulge any pertinent details about it. That is, without knowledge of the information included in the promise, the verifier can assume that the information in the promise is within a given range or that two or more promises conceal the same information (Sun et al., 2021). ZKP has significantly impacted the advancement of computer science and cryptography by incorporating randomness into conventional mathematical proof to establish the veracity of a particular claim. ZKP has two types: interactive and non-interactive, and it offers a practical solution for the blockchain's privacy protection and the authentication of encrypted transactions (Gaba et al., 2022). Suppose $Q\left(s,p\right)$ is an uncertain relationship, s is a statement and p is a witness. ZKP is a protocol, including a prover and a verifier, who share a statement s. The prover knows the witness p and $\left(s,p\right)\in Q$, and he wants to convince the verifier $\left(s,p\right)\in Q$ without revealing p's information. A ZKP protocol needs to meet three requirements: zero knowledge, the verifier knows nothing about the prover's secret p. Integrity, if the prover is telling the truth, the verifier is likely to accept it. Robustness, if there is no p to make $\left(s,p\right)\in Q$, the verifier will refuse to believe it.

With the rapid development of ZKP technology, it has been considered a reliable method to solve blockchain's information security and personal privacy problems. Currently, the most widely used ZKP technology is zero-knowledge successful non-interactive argument of knowledge (zk-SNARK). Due to the security of zk-SNARK, many cryptocurrencies such as Zerocash and Zerocoin have been successfully applied to their respective blockchain systems (Khan et al., 2023; Tang & Zhang, 2022). However, a trusted third party must initialise the traditional zk-SNARK scheme. In the process of initialization, some variable information may be leaked, and the attacker will use these leaked variables to generate unverifiable false certificates (Ni, & Zhu, 2023). Therefore, zk-SNARK needs to be optimized.

A trusted execution environment (TEE) is a unique memory region of a computer's central processing unit that establishes a secure and dependable computing environment for users at the level of the server hardware environment. Users can load sensitive data analysis or messages into the TEE protection when sensitive messages or data analysis is necessary, preserving the privacy and security of users' private information (Valadares et al., 2021). Most client applications are used in an insecure environment on the system level, whereas TEE is utilized in a secure environment. The unsafe environment is referred to as a rich execution environment (REE) since it supports various programs and full functions (Suzaki et al., 2021). To manage keys for security operations and process sensitive data or information, such as encrypting and decrypting files, TEE is mainly used. A trusted application is a program that executes inside a TEE. Even though it just has a few features, it is pretty secure (Dokmai et al., 2021). A program that runs in a REE is referred to as a client application. Client applications are used to handle the majority of user needs, sensitive files, and some sensitive tasks that require calling TEE. Multiple apps that require isolation can operate on TEE and communicate with one another wirelessly. Hardware separation technology, trusted boot and trusted control system, which may establish a secure and dependable operating environment for sensitive data information and codes to protect the privacy and accuracy of data information, make up the three primary components of TEE (Kato et al., 2021). Figure 3 depicts the TEE software architecture.

TEE can aid blockchain more effectively by boosting security, performance, and privacy concerns. Since the majority of public chain engineering projects cannot guarantee each link's high safety conditions, most links must agree to improve safety. Since the number of links is the opposite of reliability, this has led to significant reliability issues for public chain engineering projects. The TEE can guarantee that the computer running the program will not be hacked and will function normally

Figure 3. TEE architecture



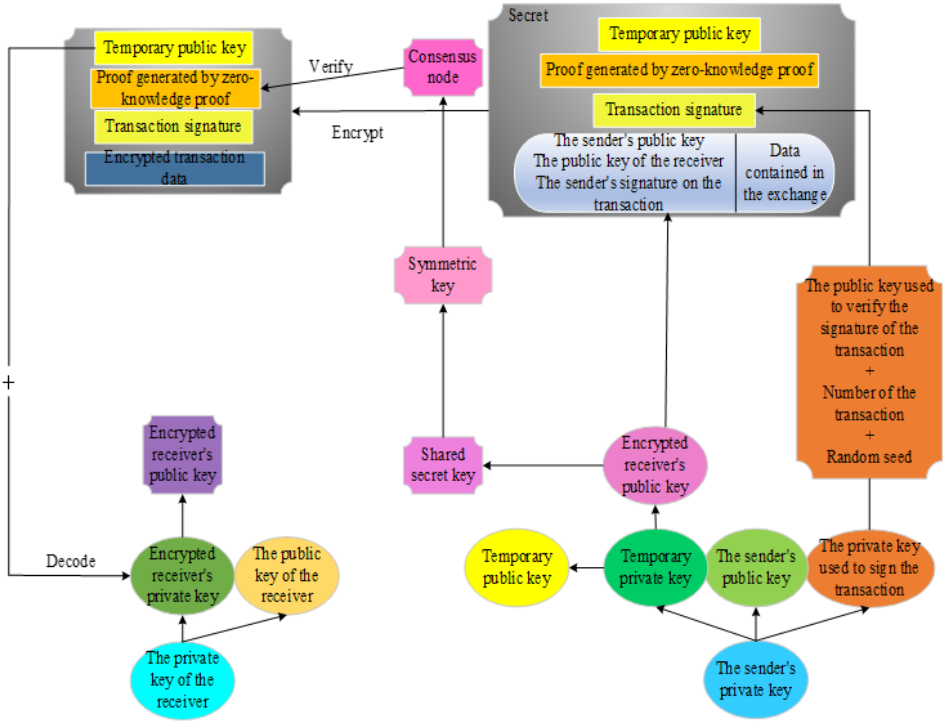
following the particular blockchain technology, considerably enhancing the quality and security of the whole network system (Zhang et al., 2021). Combining TEE and ZKP, and optimizing based on zk-SNARK, a new ZKP algorithm called TEE-ZKP algorithm is proposed to realize the security and privacy protection of blockchain (Qin et al., 2022; Xiao et al., 2022).

Information Security and Privacy Protection System Based on Blockchain

Based on ZKP and TEE, an information security and privacy protection system based on blockchain is designed, as shown in Figure 4 (Lv et al., 2021; Wang, & Li, 2021; Wu et al., 2021).

The three primary components of the blockchain-based information security and privacy protection system are the encryption and decryption process, ZKP process, and TEE protocol, as shown in Figure 4. (Mishra et al., 2021; Peng et al., 2022). Encryption mechanism is mainly used to ensure the information security of the parties in the transaction process and the confidentiality of the transaction process. First, the receiver will send the public and encrypted keys to the sender. Then the sender will generate a temporary asymmetric key pair. In order to ensure the integrity of the transaction and prevent man-in-the-middle attacks, the sender will generate another asymmetric key pair and a public key used to verify the transaction's signature. The public key is used to verify the transaction signature, the random seed is used to generate the random number, and the transaction number is hashed to generate the transaction signature to ensure the integrity of the transaction. Secondly, the sender will use the temporary private key and the encrypted public key of the receiver to construct a shared secret, and then generate an asymmetric key. The sender encrypts the transaction data (sender's public key, receiver's public key, transaction amount, sensitive information and other data) with a symmetric key to ensure the confidentiality of the transaction. Thirdly, before sending the marketing, the sender will use the ZKP technology to generate a proof A for the hidden transaction data to ensure the correctness of the transaction and prevent the double-flower trade. Finally, the sender packages

Figure 4. Information security and privacy protection system based on blockchain


Temporary public key
Proof generated by zero-knowledge proof
Transaction signature
Encrypted transaction data
Verify
Encrypt
Consensus node
Secret
Temporary public key
Proof generated by zero-knowledge proof
Transaction signature
The sender's public key
The public key of the receiver
The sender's signature on the transaction
Data contained in the exchange
Symmetric key
The public key used to verify the signature of the transaction
+
Number of the transaction
+
Random seed
+
Encrypted receiver's public key
Shared secret key
Encrypted receiver's public key
Decode
Encrypted receiver's private key
The public key of the receiver
The private key of the receiver
Temporary public key
Temporary private key
The sender's public key
The private key used to sign the transaction
The sender's private key

and uploads the encrypted ciphertext, transaction signature, certificate A and temporary public key to the blockchain. After the encrypted transaction is uploaded to the blockchain, the consensus node will verify the transaction to ensure its correctness and integrity. When the transaction is verified, it will be stored in the blockchain in encrypted form. The receiver will also generate a symmetric key through the encrypted public key and the temporary public key then decrypt the encrypted transaction with the symmetric key to obtain the plaintext of the transaction. The encrypted transaction will be loaded into the TEE if the recipient is a smart contract. The enclave will also generate a symmetric secret key to decrypt the transaction and obtain the sender's public key, private key signature and related data. Then the smart contract will verify the sender's identity according to the secret key and signature, and whether it meets the conditions for the execution of the smart contract. When the verification is passed, the relevant data obtained after decryption will be used as the input parameters for smart contract execution. Finally, the execution result of the smart contract is returned. The main function of ZKP is to generate a proof A to ensure the correctness of the transaction. In the transaction, ZKP mainly includes three aspects: the proof of the equality of transaction amount, the proof of the equality of input amount and output amount, and the proof that the transaction amount is greater than 0. TEE protects privacy in IoT access control based on smart contract. TEE can ensure that the execution of code in the enclave is not affected by external processes and, meanwhile ensure the security and confidentiality of the execution state and data.

Experimental Environment Setting

This paper verifies the feasibility of the proposed system through simulation experiments. The experimental equipment is shown in Table 1.

The Truffle framework is used to deploy and call smart contracts, a development framework based on Ethereum Solidity language. Using Ganache to develop and test local blockchain, Ganache can simulate a realistic Ethereum system, including created accounts and used Ethereum, and be used to build and test local blockchain. The server plays the role of the resource owner, the desktop computer is the consensus node, the notebook computer is the access requester, and the raspberry pie is the gateway because these devices have certain computing and storage capabilities. Meanwhile, these devices also installed an Ethereum client to convert these devices into Ethereum nodes. In this paper, Remix integrated development environment is used to write and compile smart contracts, and web3.js and Ethereum clients are connected by hypertext transfer protocol, thus deploying the compiled smart contracts. Web3.js can monitor the execution status of smart contracts, that is, access control results, by interacting with Ethereum clients. The access requester sends an access request transaction to the authentication contract through the Ethereum client and receives the returned access result from the authentication contract.

The TEE-ZKP algorithm is compared with the zero-knowledge scalable transparent argument of knowledge (zk-STARK), Bulletproof, Ligero and other ZKP algorithms. Zk-STARK is an encryption proof, which uses a hash function, hardly needs any interaction between prover and verifier, and can also resist quantum attacks. Bulletproof is a more space-efficient form of ZKP. The constructed Rank-1

Table 1. List of experimental equipment

Model	Lenovo Think Station P910
Operating system	64-bit Windows 10
Central processing unit	Intel Xeon E5-2640 v4, 2.4GHz
Memory	64GB
Hard disc drive	2TB
System for testing local blockchain	Ganache

constraint system does not need trusted settings, thus avoiding the problems of past protocol parameter generation and multiple trusted settings. Ligero is a lightweight and extensible protocol for secure multi-party computing and ZKP, which is convenient for security and privacy cooperation in blockchain and other fields. The algorithm's performance is verified by the proof generation time and verification time of the proof algorithm. The shorter the two times, the better the performance of the algorithm.

RESULTS AND DISCUSSION

Performance Analysis of Information Security and Privacy Protection System Based on Blockchain

The comparison results of proof generation time among Bulletproof, Ligero, zk-STARK and TEE-ZKP are shown in Figure 5.

From Figure 5, the proof time increases with the increase of nodes. However, TEE-ZKP algorithm is superior to other algorithms in the time of proof generation. When the experiment reaches the highest node 2^8, the generation time of TEE-ZKP algorithm is only 352ms, which is slightly higher than 311ms at the beginning of zk-STARK and Bulletproof algorithms and lower than 446ms at the beginning of Ligero algorithm.

Secondly, the verification time of the algorithm is compared, and the result is shown in Figure 6.

From Figure 6, the zk-STARK algorithm is the best in the verification time, and the final time is stable at about 8ms. The verification time of Bulletproof and Ligero algorithm is 18ms and 45ms, respectively, and the performance of Ligero algorithm is relatively poor. The verification time of the proposed TEE-ZKP algorithm is finally stable at about 15ms, 3ms and 30ms shorter than Bulletproof and Ligero algorithms and only 7ms higher than zk-STARK algorithm. Combined with the shortest proof generation time of TEE-ZKP algorithm in Figure 5, the proposed TEE-ZKP proof algorithm is effective.

Figure 5. Comparison of time required for each algorithm to generate proof

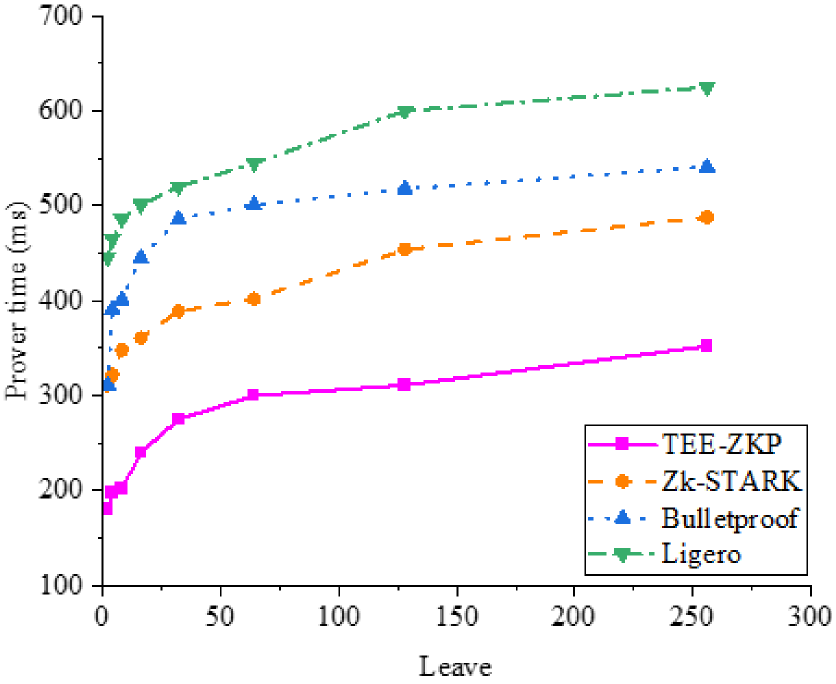
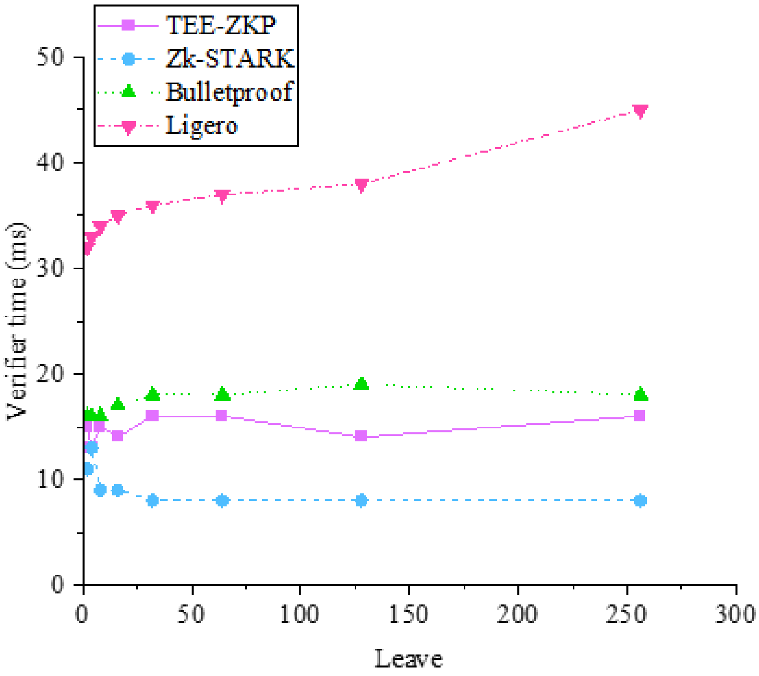


Figure 6. Comparison of verification time of each algorithm



Access Control Analysis of Information Security and Privacy Protection System Based on Blockchain

According to different types of access applicants, the network delay test of access applications between intra-domain access applicants and cross-domain access applicants, from the local gateway to IoT devices, is carried out. The results are shown in Figure 7.

According to Figure 7, the network delay or response time for users inside the domain is slightly lower than for users outside the domain. The network delay for users inside the domain is stable at around 36 ms with the rise in access requests. In comparison, the network delay for users outside the domain is stable at about 40 ms except for 30 access requests. In general, visitors' response times, whether they are from within or outside the domain, are brief—less than 60 ms.

To test the validity of the access control of this framework, the concurrent access applications with access times of 100 times, 200 times, 500 times and 1000 times are tested. The average delay of four groups of access applications was recorded in detail, and compared with the Attribute-Based Access Control (ABAC) model and the Role-Based Access Control (RBAC) model based on blockchain. These two access models are the most common and traditional access control models used to protect data security and privacy. ABAC uses blockchain technology to create, manage and implement access control policies, allowing distributed resource access. However, this scheme is not completely decentralized, and it needs an authorization center for policy execution, policy management, and policy decision points. In addition, the exchange of access control policies and access rights is publicly visible, which may violate the privacy of relevant users. RBAC is a classic and secure access and management method mode, and users can manage IoT devices through smart contracts. The results are shown in Figure 8.

From Figure 8, in the average response time of access control, TEE-ZKP increases with the increase of the number of concurrent access requests. When there are 1000 concurrent access requests, the average response time of TEE-ZKP is 330ms, the lowest is ABAC model, 299ms, and the highest

Figure 7. Access response time of access requester

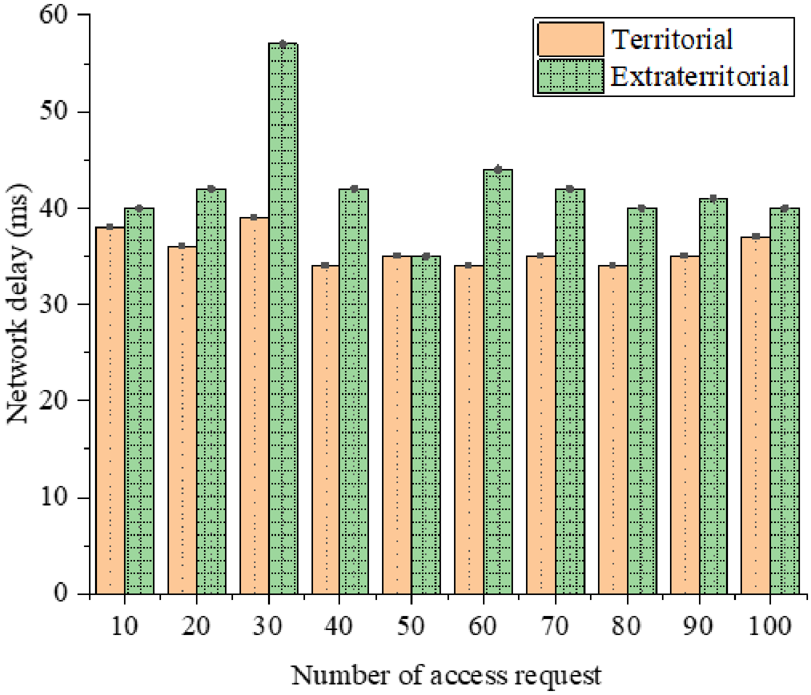
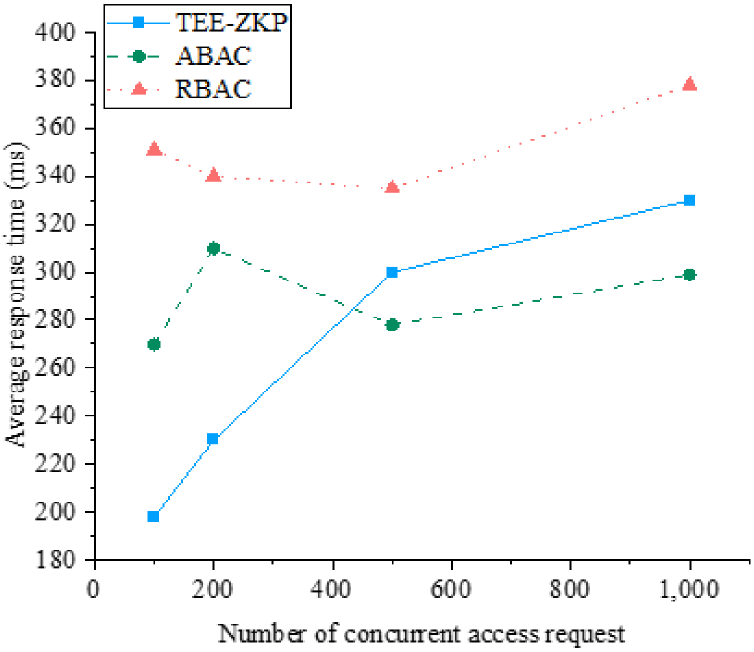


Figure 8. Comparison of average response time of access control



is RBAC model, 378 ms. When there are 100 concurrent access requests, the lowest is TEE-ZKP, which is 198 ms. Therefore, the response time of TEE-ZKP's concurrent access requests is lower when the number of visits is low. The delay time is also increasing with the increase of the number of concurrent access requests, but the overall performance is better.

Discussion

To sum up, the proposed TEE-ZKP fusion algorithm has shorter proof generation and verification time and lower access response time, which can be used to protect the information and privacy of IoT compared with other studies. Alwarafy et al. conducted a comprehensive survey on the security and privacy issues in the context of edge computing-assisted IoT, discussed the main types of attacks in edge computing-assisted IoT, and provided possible solutions, countermeasures, and related research work. They also provided several open challenges and future research directions of the paradigm of secure edge computing-assisted IoT (Alwarafy et al., 2020). This study focuses on the IoT assisted by edge computing, and discusses its security protection and privacy issues. Compared with the research in this paper, although both of them are aimed at the privacy security of the IoT, they have different starting points. The research in this paper is more inclined to use blockchain technology to protect information and privacy in IoT. Abd EL-Latif et al. proposed a new encryption mechanism of privacy protection medical care system based on IoT by using controlled alternating quantum roaming to protect patients' privacy. The simulation results show that its image encryption protocol effectively protects patients' privacy (Abd EL-Latif et al., 2020). This paper uses quantum algorithm, which is different from blockchain technology, but both studies have contributed to the privacy protection of the IoT. Yi proposed a post-quantum ring signature, and based on this, a blockchain system based on ring signature was constructed to protect users' privacy in the social IoT. Compared with the traditional social IoT, the system is safe for both traditional computers and quantum computers. In addition, the results of the blockchain system show that it is very suitable for social IoT (Yi, 2021). The object of this paper is the social IoT, which uses post-quantum technology and blockchain technology to protect users' privacy in the social IoT. It is consistent with the research results of this paper, which prove the role of blockchain technology in the information security protection of the IoT.

CONCLUSION

To study the application of blockchain technology in the information protection and privacy security of IoT, based on the basic architecture of IoT and blockchain technology, this paper explores the role of ZKP and TEE in the privacy protection and information security of the blockchain, puts forward the TEE-ZKP fusion algorithm, and designs the information security and privacy protection system of IoT based on the blockchain. Using simulation experiments to test the proposed model's validity, the following findings are made: (1) The proof generation time of the TEE-ZKP algorithm is just 352ms when it reaches the highest node 2^8 in the experiment, making it faster than other algorithms. (2) The TEE-ZKP method is ultimately stable during proof and verification at 15 ms, which is longer than the zk-STARK algorithm but still within acceptable bounds. (3) Whether a visitor is inside or outside the domain, TEE-access ZKP's response time is less than 60m in terms of access control time. While TEE-concurrent ZKP's access requests have a reduced response time, fewer accesses, and a longer latency as more requests are made concurrently, overall performance is still strong. These findings demonstrate that the suggested system model may guarantee high access management efficiency while achieving accurate and safe access control with minimal latency. This paper still has several flaws, though. The average response time of EE-ZKP will steadily increase as the number of concurrent access requests rises, which makes it slower than other algorithms and calls for improvement. Simultaneous access can benefit TEE-ZKP from further study. Future studies may also consider addressing the IoT's privacy issue at the network level and through data transmission methods.

FUNDING

This work was supported by following funding:

Project No.: 007JKY074AW. Project Title: Research on the Coupling Mechanism of Inclusive Entrepreneurship Growth Mode and Common Prosperity Realization Mode.

Project: Industry-University Cooperation and Collaborative Education Project of the Ministry of Education (22097158162822).

Project number: 22097158205119; Project name: Exploration and research on Construction of financial comprehensive Simulation Practice Base from the perspective of school-enterprise collaborative integration; Project source: Industry-school Cooperative Education Project of Ministry of Education.

REFERENCES

Abd EL-Latif, A. A., Abd-El-Atty, B., Abou-Nassar, E. M., & Venegas-Andraca, S. E. (2020). Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. *Optics & Laser Technology*, *124*, 105942. doi:10.1016/j.optlastec.2019.105942

Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 12730–12749. doi:10.1109/ACCESS.2021.3050241

Alsharari, N. (2021). Integrating blockchain technology with internet of things to efficiency. *International Journal of Technology, Innovation and Management, 1*(2), 1-13.

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet of Things Journal*, *8*(6), 4004–4022. doi:10.1109/JIOT.2020.3015432

Choi, W., Kim, J., Lee, S., & Park, E. (2021). Smart home and internet of things: A bibliometric study. *Journal of Cleaner Production*, *301*, 126908. doi:10.1016/j.jclepro.2021.126908

Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Kashif Bashir, A. (2022). A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies*, *33*(6), e3935. doi:10.1002/ett.3935

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences (Basel, Switzerland)*, *11*(10), 4580. doi:10.3390/app11104580

Dokmai, N., Kockan, C., Zhu, K., Wang, X., Sahinalp, S. C., & Cho, H. (2021). Privacy-preserving genotype imputation in a trusted execution environment. *Cell Systems*, *12*(10), 983–993. doi:10.1016/j.cels.2021.08.001 PMID:34450045

Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, *8*(14), 11717–11731. doi:10.1109/JIOT.2021.3058946

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. doi:10.1109/ACCESS.2021.3118642

Ferrag, M. A., & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet of Things Journal*, *8*(24), 17236–17260. doi:10.1109/JIOT.2021.3078072

Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., & Alazab, M. (2022). Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. *Sustainable Cities and Society*, *80*, 103766. doi:10.1016/j.scs.2022.103766

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological Forecasting and Social Change*, *163*, 120407. doi:10.1016/j.techfore.2020.120407

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain. *Research and Applications*, *2*(4), 100027. doi:10.1016/j.bcra.2021.100027

Kato, F., Cao, Y., & Yoshikawa, M. (2021). PCT-TEE: Trajectory-based Private contact tracing system with trusted execution environment. *ACM Transactions on Spatial Algorithms and Systems*, *8*(2), 1–35. doi:10.1145/3490491

Khan, R., Mehmood, A., Iqbal, Z., Maple, C., & Epiphaniou, G. (2023). Security and Privacy in Connected Vehicle Cyber Physical System Using Zero Knowledge Succinct Non Interactive Argument of Knowledge over Blockchain. *Applied Sciences (Basel, Switzerland)*, *13*(3), 1959. doi:10.3390/app13031959

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. doi:10.1016/j.cose.2021.102267

Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkiewicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management*, *62*, 102442. doi:10.1016/j.ijinfomgt.2021.102442

Li, M., Bi, X., Wang, L., Han, X., Wang, L., & Zhou, W. (2022). Text Similarity Measurement Method and Application of Online Medical Community Based on Density Peak Clustering. *Journal of Organizational and End User Computing*, *34*(2), 1–25. doi:10.4018/JOEUC.302893

Li, Y., Zuo, Y., Song, H., & Lv, Z. (2021). Deep learning in security of internet of things. *IEEE Internet of Things Journal*, *9*(22), 22133–22146. doi:10.1109/JIOT.2021.3106898

Lim, M. K., Li, Y., Wang, C., & Tseng, M. L. (2021). A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Computers & Industrial Engineering*, *154*, 107133. doi:10.1016/j.cie.2021.107133

Liu, Y., Zhang, J., & Zhan, J. (2021). Privacy protection for fog computing and the internet of things data based on blockchain. *Cluster Computing*, *24*(2), 1331–1345. doi:10.1007/s10586-020-03190-3

Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J. (2021). Analysis of using blockchain to protect the privacy of drone big data. *IEEE Network*, *35*(1), 44–49. doi:10.1109/MNET.011.2000154

Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2021). Privacy protected blockchain based architecture and implementation for sharing of students' credentials. *Information Processing & Management*, *58*(3), 102512. doi:10.1016/j.ipm.2021.102512

Mohammed, I. A. (2021). The interaction between artificial intelligence and identity and access management: An empirical study. International Journal of Creative Research Thoughts (IJCRT). *ISSN*, *2320*(2882), 668–671.

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., Dobre, O., & Poor, H. V. (2021). 6G Internet of Things: A comprehensive survey. *IEEE Internet of Things Journal*, *9*(1), 359–383. doi:10.1109/JIOT.2021.3103320

Ni, N., & Zhu, Y. (2023). Enabling zero knowledge proof by accelerating zk-SNARK kernels on GPU. *Journal of Parallel and Distributed Computing*, *173*, 20–31. doi:10.1016/j.jpdc.2022.10.009

Peng, T., Guan, K., & Liu, J. (2022). A privacy-preserving mobile crowdsensing scheme based on blockchain and trusted execution environment. *IEICE Transactions on Information and Systems*, *105*(2), 215–226. doi:10.1587/transinf.2021BCP0001

Qin, L., Zhang, G., & You, L. (2022). Application of CSK encryption algorithm in video synergic command systems. *Journal of Organizational and End User Computing*, *34*(2), 1–18. doi:10.4018/JOEUC.20220301.oa1

Sekar, S., Solayappan, A., Srimathi, J., Raja, S., Durga, S., Manoharan, P., & Tunze, G. B. et al. (2022). Autonomous transaction model for e-commerce management using blockchain technology. *International Journal of Information Technology and Web Engineering*, *17*(1), 1–14. doi:10.4018/IJITWE.304047

Shu, L., Ferrag, M. A., & Choo, K. K. R. (2021). Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives. *IEEE/CAA Journal of Automatica Sinica, 8*(9), 1477-1499.

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network*, *35*(4), 198–205. doi:10.1109/MNET.011.2000473

Suzaki, K., Nakajima, K., Oi, T., & Tsukamoto, A. (2021). Ts-perf: General performance measurement of trusted execution environment and rich execution environment on intel sgx, arm trustzone, and risc-v keystone. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 133520–133530. doi:10.1109/ACCESS.2021.3112202

Tang, Y., & Zhang, P. (2022). The Impact of Virtual Integration on Innovation Speed: On the View of Organizational Information Processing Theory. *Journal of Organizational and End User Computing*, *34*(1), 1–20. doi:10.4018/JOEUC.298702

Valadares, D. C. G., Will, N. C., Caminha, J., Perkusich, M. B., Perkusich, A., & Gorgônio, K. C. (2021). Systematic literature review on the use of trusted execution environments to protect cloud/fog-based Internet of Things applications. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 80953–80969. doi:10.1109/ACCESS.2021.3085524

Wang, B., & Li, Z. (2021). Healthchain: A privacy protection system for medical data based on blockchain. *Future Internet*, *13*(10), 247. doi:10.3390/fi13100247

Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing Communications and Applications*, *17*(2s), 1–17. doi:10.1145/3408321

Xiao, Q., Li, S., Zhang, X., Zhang, F., Yue, Q., & Wan, S. (2022). Deconstructing online hospitality review systems: User quality experience toward design features. *Journal of Organizational and End User Computing*, *34*(2), 1–17. doi:10.4018/JOEUC.292523

Yi, H. (2021). Secure social internet of things based on post-quantum blockchain. *IEEE Transactions on Network Science and Engineering*, *9*(3), 950–957. doi:10.1109/TNSE.2021.3095192

Zeadally, S., Das, A. K., & Sklavos, N. (2021). Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things*, *14*, 100075. doi:10.1016/j.iot.2019.100075

Zhang, Q., Zhong, H., Shi, W., & Liu, L. (2021). A trusted and collaborative framework for deep learning in IoT. *Computer Networks*, *193*, 108055. doi:10.1016/j.comnet.2021.108055

Zhao, L., Jiang, J., Feng, B., Wang, Q., Shen, C., & Li, Q. (2021). Sear: Secure and efficient aggregation for byzantine-robust federated learning. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 3329–3342. doi:10.1109/TDSC.2021.3093711

Shuya Fang received the B.Sc. degree in engineering from North Minzu University,China, in 2010, the M.Sc. degree in management from Zhengzhou University,China, in 2013,and Ph.D degree in management from INHA University, Korea. She is a lecturer in School of Economics and Management of Zhoukou Normal University, and her research interests include blockchain technology application and sustainability.