Research on Privacy Protection in IoT System Based on Blockchain

Shiping Fan, Liang Song and Chunyan Sang

September 12, 2019

Research on Privacy Protection in IoT System Based on Blockchain[⋆]

Shiping Fan[1], Liang Song[1], and Chunyan Sang[2]

[1] School of Communication and Information Engineering,Chongqing University of Posts and Telecommunications, Chongqing 400065, China
fansp@cqupt.edu.cn,songliang159@gmail.com

[2] School of Software Engineering,Chongqing University of Posts and Telecommunications, Chongqing 400065, China
sangcy@cqupt.edu.cn

Abstract. The Internet of Things (IoT) is an important area of next-generation information technology, and its value and significance are widely recognized. While providing development opportunities, the IoT also presents major challenges. Security and privacy have become severe issues that cannot be ignored in the development of the IoT in this paper, so we will propose an IoT information security protection scheme based on blockchain technology. The scheme utilizes the security features of the blockchain combined with the AES encryption algorithm to encrypt the original IoT information, and the ciphertext distributed storage can effectively solve the IoT data storage problem. Experiments shown in this scheme could reduce the operation and credit cost of centralized network. At the same time, the blockchain-based IoT information security protection scheme combined with cryptography knowledge can effectively solved the big data management and trust faced in the development of the IoT, security and privacy issues.

Keywords: Blockchain · IoT information security · IoT data storage· IPFS · Access control.

[⋆] This work is supported by the National Natural Science Foundation (Grant No. 61772099, 61772098); the Program for Innovation Team Building at Institutions of Higher Education in Chongqing (Grant No.CXTDG201602010); Chongqing Science and Technology Innovation Leadership Support Program (Grant No. CSTC-CXLJRC201917); the University Outstanding Achievements Transformation Funding Project of Chongqing (Grant No. KJZH17116); the Artificial Intelligence Technology Innovation Important Subject Projects of Chongqing (cstc2017rgzn-zdyf0140); The Innovation and Entrepreneurship Demonstration Team Cultivation Plan of Chongqing (cstc2017kjrc-cxcytd0063); the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjAX0270, Grant No. cstc2018jcyjA0672, Grant No. cstc2017jcyjAX0071); the Industry Important Subject Projects of Chongqing(Grant No. CSTC2018JSZX-CYZTZX0178, Grant No. CSTC2018JSZX-CYZTZX0185)

1 Introduction

As an important field of new generation information technology, the IoT has its universal recognition of value and significance. Industrial equipment, automobiles, smart home and other items are connected to each other through the network and generating a large amount of data, combined with powerful data analysis capabilities which is expected to change the way of production and life, while generating enormous social and commercial value[1, 2]. However , while the IoT providing opportunities for development, the IoT has also brought significant challenges which security and privacy have become issues that cannot be ignored in the development of the IoT[3]. The blockchain integrates technologies such as distributed data storage, peer-to-peer transmission, consensus mechanism, and encryption algorithm. It is expected to solve the weakness of IoT security, reduce the operation and credit cost of centralized network, and improve operational efficiency and industrial asset utilization. To enhance the value of the IoT system[4, 5].

Blockchain is a mode for constructing and managing transaction processing through transparent and trusted rules in a peer-to-peer network environment. It has distributed peer-to-peer, chained data blocks and defenses. Typical characteristics of forgery and tamper resistance, transparency and reliability, and high reliability[6]. Gai, K. proposed distributed power energy trading in the peer-to-peer network environment using blockchain and transparent and credible rules to construct and manage transaction processing models[7]. Blockchain can provide two application capabilities for the IoT: one is to provide infrastructure for computing, storage, network and platform resources through peer-to-peer networks, and the other is to manage, query and analyze data in peer-to-peer networks[8]. Reference [9,10] proposed model is a distributed cloud architecture based on blockchain technology, which provides low-cost, secure, and on-demand access to the most competitive computing infrastructures in an IoT network.Zhu, L. proposed a controllable blockchain data management (CBDM) model that can be deployed in a cloud environment[11].

Combining the unique technical characteristics of the blockchain, this paper proposes a blockchain-based IoT information security protection scheme, which can effectively solve the problems of big data management, trust, security and privacy faced in the development of the IoT. Blockchain-based protection schemes provide trust, ownership records, transparency, and communication support for the IoT, enabling scalable device coordination, building efficient, trusted, and secure distributed IoT networks, and deploying massive amounts of devices Data-intensive applications running on the network, while providing effective protection for user privacy. In this paper, the combination of Advanced Encryption Standard (AES) algorithm and smart contract is applied to the IoT information security platform based on blockchain. The AES algorithm is used to directly process the ciphertext without divulging the real plaintext, thus ensuring the confidentiality of the data.

2 Blockchain solves IoT information security requirements

2.1 IoT Information Security Requirements

Security is the most important issue in IoT applications. The traditional IoT information security protection is protected from the IoT perceptual layer, the IoT network layer and the IoT application layer[12]. However, by controlling the availability of the network,inputting erroneous data into the network, illegally accessing personal privacy information and other means to attack the IoT system to destroy the security of the IoT, the existing security protection technology is difficult to solve [13]. In this paper, we propose the IoT and blockchain solution for IoT information security. The security requirements of the solution include: (1) data auditable and tamper-proof, (2) identity authentication, (3) privacy protection, and (4) data access control. (5) tracking violations.

2.2 Applicability of Blockchain to IoT

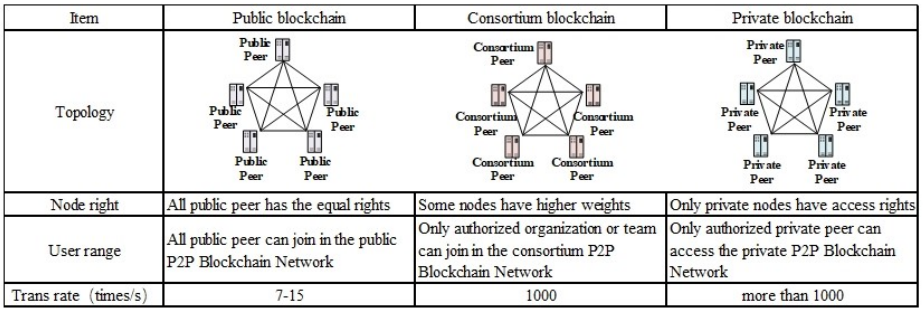
Blockchain classifications include public blockchain, consortium blockchain, and private blockchain[14, 15]. A comparison of each blockchain is shown in Figure 1. Based on the requirements of the IoT, considering the large storage capacity of image, audio, video and other multi-data information content, the appropriate framework for the blockchain is to "build blocks on the internal blockchain platform and store the content itself in the external database." The scheme proposes efficient, secure authentication, privacy protection, and multi-signature-based conditional traceability methods to easily retrieve IoT data licenses, usage controls, and constraint information from the blockchain.

According to the requirements of the management of IoT data, the blockchain can only be used by authorized or multi-part administrators to manage content in a credible and tamper-proof manner, providing credible content violation traceability, and reading, writing or auditing operations must comply with access control strategy. Therefore, according to the above analysis, in this paper, we choose the consortium blockchain as the IoT information management, which is used to store the original content source for anti-counterfeiting evidence and violation of tracking, and then the content itself, content ownership, rights holder,content obligations and security requirements can be included in the consortium blockchain and authorized processing.

3 Blockchain solves IoT information security

3.1 Blockchain solution to solve the problem of information security of the IoT

This paper proposes a blockchain-based IoT information security protection scheme (IoTChain), which can effectively protect the security of IoT devices


Public Peer
Public Peer
Public Peer
Public Peer
Public Peer
Consortium Peer
Consortium Peer
Consortium Peer
Consortium Peer
Consortium Peer
Private Peer
Private Peer
Private Peer
Private Peer
Private Peer

Item	Public blockchain	Consortium blockchain	Private blockchain
Topology			
Node right	All public peer has the equal rights	Some nodes have higher weights	Only private nodes have access rights
User range	All public peer can join in the public P2P Blockchain Network	Only authorized organization or team can join in the consortium P2P Blockchain Network	Only authorized private peer can access the private P2P Blockchain Network
Trans rate（times/s）	7-15	1000	more than 1000

Fig. 1. Comparison of different blockchains

to collect information, and can serve legitimate users in a correct way, providing reliable, high levels of content protection and illegal content are traceable.

In the proposed IoTChain, considering that the information storage of voice, image, video and other IoT data needs a large amount of memory, combined with the special situation of the Internet of things, we used two isolated blockchain application interfaces to store the data of the IoT.Store the original information and the original information key of IoT data respectively.By using this chain structure, the memory size problem of blockchain itself can be solved, and the access control problem can be solved by trusted authentication.

3.2 Fusion Model of Blockchain and IoT

The blockchain and IoT fusion framework proposed in this paper can be divided into four layers, from bottom to top: perception layer, network layer, blockchain layer and application layer. As shown in Figure 2, the perceptual layer and the network layer provide the basic hardware environment and communication-related equipment facilities for the blockchain and the IoT. As an intermediate layer, the blockchain uses the hardware resources of communication and infrastructure to provide trust or consensus support mechanisms or services for IoT applications. The application layer leverages the services provided by the blockchain layer to enhance its security and privacy capabilities. The perception layer is the bottom layer of the IoT. It is the core capability to realize the perception of the IoT. It mainly solves the problem of data acquisition and connection in the biological world and the physical world[16, 17]. The most commonly used radio frequency identification (RFID) technology is a non-contact automatic identification technology, which automatically recognizes target objects and acquires relevant data through radio frequency signals. The identification process does not require manual intervention and can work in each a harsh environment. RFID technology recognizes high-speed moving objects and recognizes multiple labels at the same time, making operation quick and easy.

The network layer mainly solves the problem of long-distance transmission of data obtained by the sensing layer[17]. Wireless Sensor Network (WSN) is a

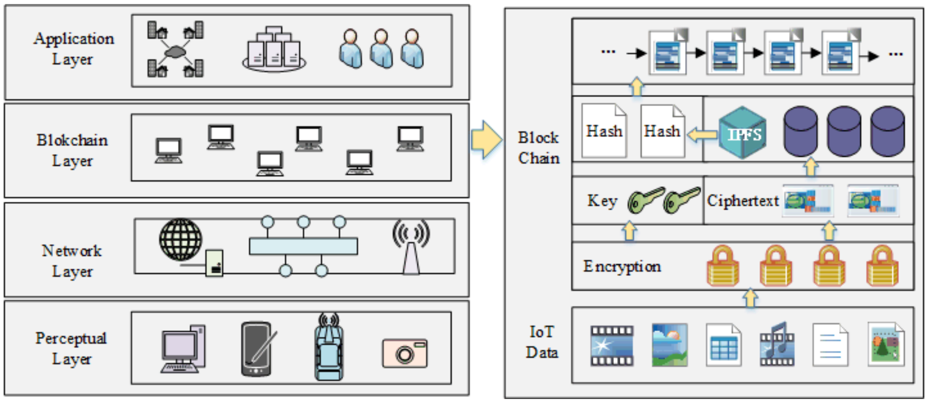


Fig. 2. Blockchain and IoT fusion model

network information system that integrates distributed information collection, information transmission and information processing technologies. It is low-cost, miniaturized, low-power and flexible. And the characteristics that are suitable for moving targets are widely valued and are important technologies related to national economic development and national security. The IoT is the ultimate perception of the entire material world through a variety of sensors and wireless sensor networks that are spread across all corners and objects.

Blockchain is a distributed network environment that constructs traceable blockchain data structures through transparent and trusted rules to implement and manage transaction processing modes. It has distributed peer-to-peer, chained data blocks and anti-counterfeiting. And typical features of three aspects: tamper resistance, transparency and reliability. The blockchain layer combines the technical characteristics of the blockchain to effectively solve the problems of big data management, trust, security and privacy faced in the development of the IoT. This layer architecture provides trust, ownership records, transparency and communication support for the IoT, enabling scalable device coordination, building an efficient, trusted, secure distributed IoT network, and deploying a massive network of devices. Data-intensive applications provide effective protection for user privacy.

The IoT application layer is a rich IoT-based application that interfaces the IoT with users, including people, organizations, and other systems. It combines with industry needs to realize the intelligent application of the IoT, and is also the fundamental goal of the development of the IoT. The industry characteristics of the IoT are mainly reflected in its application areas. At present, green agriculture, industrial monitoring, public safety, urban management, telemedicine, smart home, intelligent transportation and environmental monitoring have all tried the IoT applications.

3.3 Out-of-chain database of blockchain and IoT integration

The original information such as images, sounds and videos collected by the IoT occupies a large amount of memory. This paper proposes an external chain database for storing data information in conjunction with a chained data structure of a blockchain. The database outside the chain mainly stores the raw data information collected by the IoT device. The blockchain is used as an unchangeable database to store index values of raw data information, and the data is queried by index values. Index values can only be obtained after authorization.

4 IoT information security protection model infrastructure based on blockchain

4.1 Data storage module

The Inter Planetary File System (IPFS) is a peer-to-peer distributed files system that seeks to connect all computing devices with the same system of files. IPFS is a network transport protocol designed to create persistent and distributed storage and shared files. IPFS is a decentralized storage network based on blockchain technology and is a content-addressable peer-to-peer hypermedia distribution protocol. The nodes in the IPFS network will form a distributed file system[18].IPFS is a distributed file system which synthesizes successful ideas from previous peer-to-peer systems, including DHTs, BitTorrent, Git, and SFS, IPFS could even evolve the web itself[19]. Each file is uploaded to the network

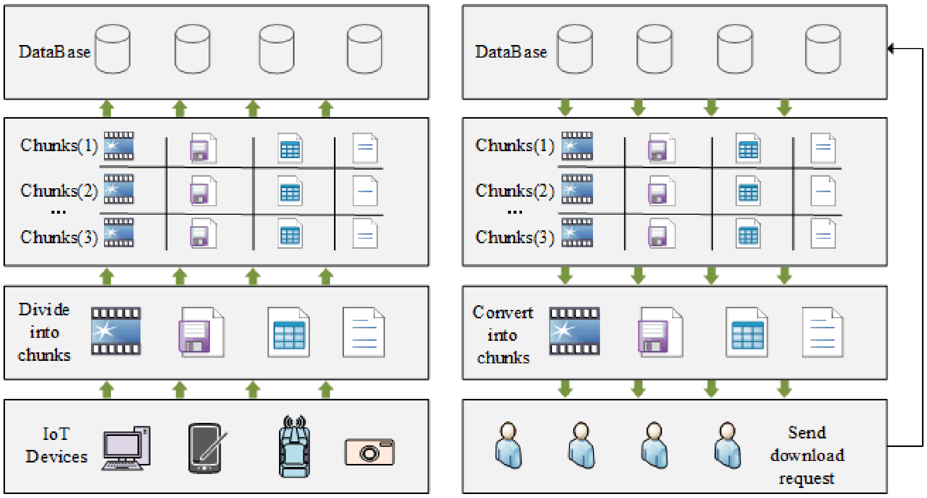


Fig. 3. IPFS file upload and download

and is hashed and a digital fingerprint is generated. IPFS deletes files with the same hash value through the network, and compares the hash values to determine which files are redundantly duplicated, and minimizes redundant files from the root cause.When searching for a file, the hash value of the file can be used to find the file where the file is stored in the network and find the required file[20].

This paper proposes a distributed and reliable storage of IoT data information based on the combination of IPFS and encryption algorithm. It solves the problem of IoT data information storage, while considering the security and non-tampering of IoT information. The IoT information is stored in the IPFS system, and the returned hash value is encrypted to store the ciphertext in the blockchain. Authorized users can obtain the hash value of the unique index stored in the IPFS system content through the smart contract for permission verification.The user access authority is determined through the smart contract, and the flow is shown in Figure 3. The response rule is preset in the smart contract. When the user needs to access the data information, a transaction needs to be initiated, and other nodes in the blockchain verify the transaction, and when the verification passes and the preset access rule is met, the authorization can be obtained. Obtain the key and block header data of the IoT data information, use the key decryption to obtain the index information, and obtain the original information through the index.

4.2 Data cryptographic module

AES is a symmetric cipher that processes data in128-bit blocks. It supports key sizes of 128, 192, and 256bits and consists of 10, 12, or 14 iteration rounds, respectively. Each round mixes the data with around key, which is generated from the encryption key. Decryption inverts the iterations resulting in a partially different data path.

The cipher maintains an internal, 4-by-4 matrix of bytes, called state, on which the operations are performed. Initially state is filled with the input data block and XORed with the encryption key. Regular rounds consist of operations called sub bytes, shift rows, mix columns, and add round key. The last round bypasses mix columns[21].

Sub bytes is an invertible, nonlinear transformation. It uses 16 identical 256-byte substitution tables (S-box)for independently mapping each byte of state into another byte. S-box entries are generated by computing multiplicative in-verses in galois field GF(2^8) and applying an affine trans-formation. Sub bytes can be implemented either by computing the substitution or using table lookups[22].

5 Blockchain for IoT information security

In this paper, we use the AES encryption algorithm, which has the advantages of simple, parallel computing, error not passing, and not easy to attack (error transmission). We performed a performance test on AES, and the test results are shown in Figure 4. The test environment of the desktop CPU is i5-8300H 2.3GHz memory size RAM 16GB. From the test results, it can be seen whether

AES encryption or decryption is suitable for the use of IoT information security scenarios.

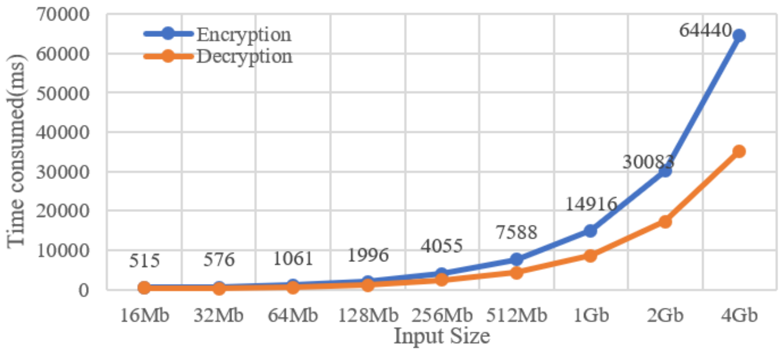
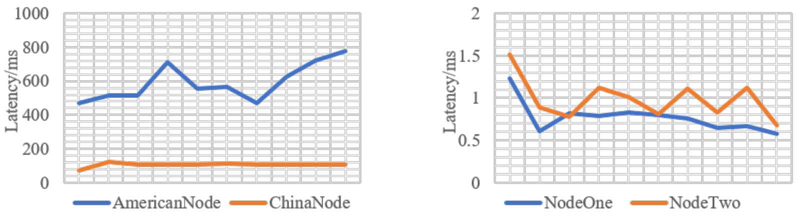


Fig. 4. AES encryption and decryption rate

In IoTChain we built a private IPFS network for information storage as a storage system for IoTChain. The simulation test results of the storage system performance of IoTChain are shown in the Figure 5. Figure (a) is the delay of the node joining the public IPFS system, and Figure (b) is the delay of the node joining the IoTChain network. It can be seen that the average delay of the node joining the network is 1.54ms, and the average delay of the node that can be added to the network by b is 92.96ms, which is superior to the public network IoTChain storage system. We uploaded the data information to the IoTChain storage system, and the lena image used in this experiment was used for simulation experiments. Gets the hash value of the file returned by the IoTChain storage system. The hash value is encrypted by the AES encryption algorithm, and the encryption result is shown in Table 1. We deployed smart



(a) Public Node

(b) IoTChain Node

Fig. 5. Delay of node joining network

Table 1. Data upload to IPFS and ciphertext upload to Blockchain

Key	Value
ImageHash in IPFS	QmaHutoUgYZF3Lepfs5wBNKHU8ij7VCAf6ho8VH38NfvMX
Key seed	w9oMoe9TYvbPb0yRfuhjKw==
Encrypted of ImageHash	NBv1TgHNsRrEIIHCItOKGxw2BuLbzG19OB33DJ7JFz7YkE2hyT9xotkR0WNgxTSA
Ethereum contract address	0xa6b4c6cf1db87fd5b2fa25118dae580248322d342bd30a61d078d3e079674853
Decrypted of ImageHash	QmaHutoUgYZF3Lepfs5wBNKHU8ij7VCAf6ho8VH38NfvMX
Transaction hash	0xc81bc1fcb8e766cea2e0f2b8c0d151118c3bc1d5d2be752895c3853685470c67
Status	Success
Block	5543565?605097 Block Confirmations
Timestamp	60 days 20 hrs ago (May-06-2019 06:49:31 AM +UTC)
From	0x7e5b7345f55797733dd13991e06d556efe67affb?
To	Contract 0x3f74edd5d2c81df73b0170f22ce7d25ef7da9191?
Input	@ NBv1TgHNsRrEIIHCItOKGxw2BuLbzG19OB33DJ7JFz7YkE2hyT9xotkR0WNgxTSA?

contracts on the Ropsten Testnet test network for performance and functional testing. The main purpose of the smart contract is to permanently store the AES encrypted ciphertext on the blockchain. The contract deployment address is shown in Table 1.

6 Conclusion

IoT information security is a key issue in the development of the IoT. This paper proposed a new mode of IoT information security management based on blockchain. We named it IoTChain, which supports large-scale secure storage of IoT information data, and can authorized legitimate users provide access services. In the IoTChain solution, we used the blockchain to store the encrypted summary information of the original data, and took into account the large-capacity IoT data information, such as images, audio or video captured by the device. We used external flexibility to store raw data information and created a hash id of the content itself and a link to the blockchain. In the IoTChain solution, we proposed efficient and secure authentication, private protection and multi-signature-based conditional traceability methods, so accessed permissions, controlled and constraint information can be easily retrieved from the blockchain. Analysis and performance evaluations show that the IoTChain solution provides reliable, secure, efficient and tamper-proof data information content services. In the future, we will strengthen our work to support the management and trading of IoT data information in the Ethereum-based currency.

References

1. Xu, L.D., E.L. Xu, and L. Li, Industry 4.0: state of the art and future trends. International Journal of Production Research, 2018. 56(8): p. 2941-2962.
2. Al-Fuqaha, A., et al., Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. Ieee Communications Surveys and Tutorials, 2015. 17(4): p. 2347-2376.
3. Jing, Q., et al., Security of the Internet of Things: perspectives and challenges. Wireless Networks, 2014. 20(8): p. 2481-2501.

4. Christidis, K. and M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things. Ieee Access, 2016. 4: p. 2292-2303.
5. Kshetri, N., Can Blockchain Strengthen the Internet of Things? It Professional, 2017. 19(4): p. 68-72.
6. Zheng, Z.B., et al., Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 2018. 14(4): p. 352-375.
7. Gai, K., et al., Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. Ieee Transactions on Industrial Informatics, 2019. 15(6): p. 3548-3558.
8. Zanella, A., et al., Internet of Things for Smart Cities. Ieee Internet of Things Journal, 2014. 1(1): p. 22-32.
9. Sharma, P.K., M.-Y. Chen, and J.H. Park, A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. Ieee Access, 2018. 6: p. 115-124.
10. Gai, K., et al., Security and Privacy Issues: A Survey on FinTech, in Smart Computing and Communication, Smartcom 2016. 2017. p. 236-247.
11. Zhu, L., et al., Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems-the International Journal of Escience, 2019. 91: p. 527-535.
12. Khan, M.A. and K. Salah, IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems-the International Journal of Escience, 2018. 82: p. 395-411.
13. Allam, Z. and Z.A. Dhunny, On big data, artificial intelligence and smart cities. Cities, 2019. 89: p. 80-91.
14. Tschorsch, F. and B. Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. Ieee Communications Surveys and Tutorials, 2016. 18(3): p. 2084-2123.
15. Pustisek, M. and A. Kos, Approaches to Front-End IoT Application Development for the Ethereum Blockchain, in 2017 International Conference on Identification, Information and Knowledge in the Internet of Things, R. Bie, Y. Sun, and J. Yu, Editors. 2018. p. 410-419.
16. Atzori, L., A. Iera, and G. Morabito, The Internet of Things: A survey. Computer Networks, 2010. 54(15): p. 2787-2805.
17. Gubbi, J., et al., Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems-the International Journal of Escience, 2013. 29(7): p. 1645-1660.
18. Botta, A., et al., Integration of Cloud computing and Internet of Things: A survey. Future Generation Computer Systems-the International Journal of Escience, 2016. 56: p. 684-700.
19. Chen, Y., et al., An improved P2P File System Scheme based on IPFS and Blockchain, in 2017 Ieee International Conference on Big Data, J.Y. Nie, et al., Editors. 2017. p. 2652-2657.
20. Wang, S., Y. Zhang, and Y. Zhang, A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. Ieee Access, 2018. 6: p. 38437-38450.
21. Hasan, H.R. and K. Salah, Combating Deepfake Videos Using Blockchain and Smart Contracts. Ieee Access, 2019. 7: p. 41596-41606.
22. Bogdanov, A., D. Khovratovich, and C. Rechberger, Biclique Cryptanalysis of the Full AES, in Advances in Cryptology - Asiacrypt 2011, D.H. Lee and X.Y. Wang, Editors. 2011. p. 344-+.