Computers and Electrical Engineering 72 (2018) 266–273

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Towards decentralized IoT security enhancement: A blockchain approach☆

Yongfeng Qian[a], Yingying Jiang[b], Jing Chen[c], Yu Zhang[b], Jeungeun Song[d], Ming Zhou[e,g,*], Matevž Pustišek[f]

[a] School of Computer Science, China University of Geosciences, Wuhan, China
[b] School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China
[c] School of Cyber Science and Engineering, Shenzhen Institute of Wuhan University, Wuhan University, Wuhan 430072, China
[d] Department of Electrical and Computer Engineering, The University of British Columbia, Canada
[e] Insititue of New Energy, Wuhan, China
[f] Laboratory for Telecommunications, Faculty of Electrical Engineering, University of Ljubljana, Slovenia
[g] School of Energy and Power Engineering, Huazhong University of Science and Technology, Wuhan 430074, China

ARTICLE INFO

Article history:
Received 8 January 2018
Revised 31 August 2018
Accepted 31 August 2018
Available online 28 September 2018

Keywords:
IoT
Blockchain
Security management

ABSTRACT

With the rapid development of internet of things (IoT), it has brought great convenience to users in different fields, such as smart home, smart transportation and so on. However, it also carries potential security risks. In order to solve this challenge, in this paper, we first introduce three layers of IoT, i.e., perception layer, network layer and application layer, then corresponding security problems of three layers are introduced. Second, we propose a high-level security management scheme based on blockchain for different IoT devices in the full life cycle. Finally, we give open research problems and future work.

1. Introduction

In recent years, with constant upgrade of terminal devices and development of new network technologies [1], internet of things (IoT) has become popular [2]. It is estimated that the scale of IoT will reach 50 billion devices in 2020. The interconnections of massive terminal devices bring great convenience to people, such as smart transportation, smart home [3] and battlefield environments [4], etc. However, there are potential risks that are also brought by IoT. For instance, moving vehicles that are connected via advanced cooperative communication are expected to form an open internet of vehicles (IoV) [5], which is a representative IoT system. Without proper protection of security measures, the deployment of IoT will not be realized [6].

Due to the profound influence, we should pay more attention to the security problems of IoT [7]. At present, the research on IoT security is heating up [8]. Kim et al. [9] introduced the security protocol problem in the IoT, described the encrypted DoS attack strategy, and implemented it in multiple IoT protocols. However, with the help of encryption, it is likely not suitable for mobile devices which do not have enough storage and computing resources. Thus, the lightweight security measures are required. Usman et al. [10] designed a lightweight encryption method, which called SIT. When used in another

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. M. Hassan.

* Corresponding author.
E-mail address: mingzhou.hust@gmail.com (M. Zhou).

https://doi.org/10.1016/j.compeleceng.2018.08.021
0045-7906/

Table 1
Existing work.

Exsisting Work	Asset Tracking	Specific Application	Communication Platform Security	(Lightweight) Blockchain-based architecture for IoT	Managing IoT devices
[16]	*	–	–	–	–
[17]	–	*	*	–	–
[15]	–	–	–	*	–
[18]	–	*	–	–	–
[19]	–	–	–	*	–
[21]	–	*	–	–	–
[22]	–	–	–	*	–
[23]	–	–	–	–	*
[24]	–	–	–	–	*

scenario, however, there will be different security problems. Mejri et al. [11] summarized the security problems appeared in the Internet of vehicles, and gave the possible encryption solutions. Zhang et al. [12] described the security problems in smart city, and introduced the possible solution. The security and privacy problems of wireless mobile networks were summarized in [13].

According to the above discussion, much work has been made for the research on IoT security. However, the research on IoT security is still in the early stages, and research on asset management for IoT terminal devices in full life cycle has not fully been taken into consideration. In the meantime, as an emerging technology, blockchain technology gradually arouses attention of academia and industry. Blockchain technology is based on a decentralized peer-to-peer network, combines encryption technology, time-series data, and consensus mechanisms, and thus realizes the traceability and verification of data. In the meantime, privacy protection and sharing are realized [14]. Currently, many researchers have begun to study blockchain technology applied for IoT. However, most of the research is based on establishment of protocol, blockchain has not been applied specifically to the full life cycle of IoT. The work in [15] described a lightweight blockchain-based IoT architecture. There are some more work in allusion to application of blockchain in IoT. For example, according to the work of Christidis et al. [16] and Biswas et al. [17], the applications of blockchain in IoT were put forth, however, only one application, i.e., automatic contract execution, was considered in application scene. How to solve safe asset management and traceability has not been taken into consideration yet. The blockchain based lightweight safety and privacy protection problem was put forth in allusion to a smart home in [18]. Similarly, only one specific case (i.e., smart home) is taken into consideration. Other IoT scenarios (significantly different from smart home, such as smart power grids) are not covered. Dorri et al. [19] put forth the optimized blockchain to relieve complicated computation and bandwidth overhead brought by traditional blockchain, and requirements on privacy protection and security were guaranteed. However, there has been no consideration of security problems of IoT terminals in the life cycle [20]. In [21], the realization mode of E-business was introduced based on blockchain and P2P trade, however, security problems applied to this type of IoT E-business have not been taken into consideration. In [22], IoT services driven by blockchain were given along with four typical frameworks. However, IoT database storage and IoT terminal management have not been taken into consideration. In [23], the IoT system was built on blockchain, and the blockchain is adopted to control and configure IoT devices. However, the blockchain ledger problem of IoT devices has not been taken into consideration. In [24], blockchain technology was adopted to realize ownership authentication for IoT devices under cloud computing, however, traceability management on data of IoT devices has not been taken into consideration. In [25], the authors utilized blockchain to realize supply chain.

From the Table 1, we can see that blockchain has been applied to the IoT in the last two years. Most of these exciting works focus on how to make use of blockchain to manage assets, ensure the security of communication platform, build lightweight architecture for IoT and managing IoT devices or specific applications (e.g., intelligent services, smart city and intelligent medica). These works use the advantage of blockchain centralization to design a fair and credible management platform or key distribution platform without third party. It break through the limitations of the third party centered, and achieve the high efficiency of processing. However, these works do not consider the threat traceability of IoT terminal life cycle. Furthermore, the life cycle of IoT terminal devices (e.g., different sensors or mobile devices) is different. Thus, in the life cycle of these terminals, how to achieve effective threat traceability can help to avoid unnecessary leakage of security and privacy issues in the actual deployment of devices for IoT. However, due to the different terminal life cycle, centralization is usually used to trace the source, which leads to the waste of resources. Therefore, how to use blockchain to deal with it is a challenge problem.

We first introduce the services acquisition of IoT device. The IoT device include vehicles, cameras, mobile phones, bracelets and other devices. These IoT devices can be accessed to the network through cellular network or WiFi, and obtain services at remote cloud [26,27]. In fact, service providers can use fog computing or edge computing to provide users with low latency services in order to ensure the quality of experience (QoE) of users [28]. For example, in the internet of vehicles, roadside units (RSUs) can be regarded as a fog node to provide services for vehicle users [29]. Though the IoT provides convenient services for users, it will also bring security problems.

Utilizing blockchain to enhance the security of IoT is shown in Fig. 1. From the Fig. 1, we can see that the blockchain is applied to the threat traceability of the IoT devices, which involves the interaction between IoT devices and network

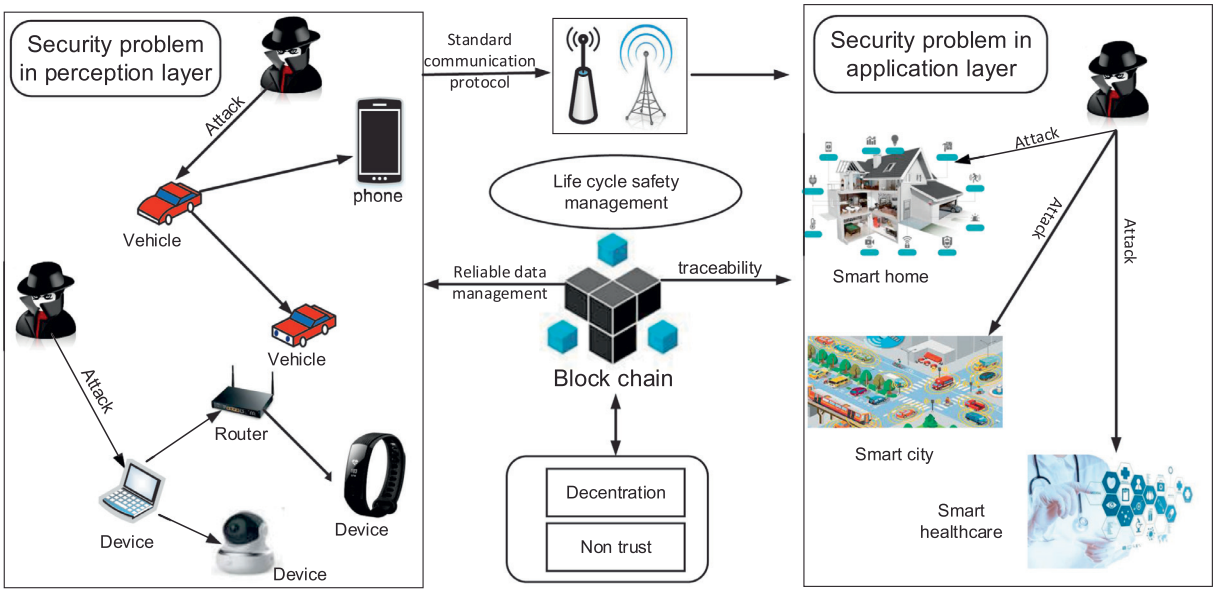

Fig. 1. Blockchain enhanced IoT security architecture.

transmission, as well as between IoT devices and cloud. For the IoT devices and network transmission, the problems include how to identify malicious hot spots, malicious terminal access, abnormal traffic monitoring, etc. For the IoT device and cloud, the problems include how to achieve identity authentication, etc. In view of the above problems, the implementation of traditional security measures usually requires trusted third party, which results in resource consumption. Therefore, the technology of blockchain can be applied to realize the implementation of the above security policy without the third party. For example, the identity authentication mechanism between the IoT device and the cloud may require third parties to distribute the key. Under the guarantee of the blockchain technology, it can realize the authentication without third parties, save the user authentication time, and bring the high QoE to the user.

Therefore, this paper focuses on utilizing blockchain technology to establish the security system for IoT terminals in full life cycles. In other words, with IoT as support and blockchain technology as the main method, IoT asset database that faces massive devices in full life cycle management is built into the platform layer. Whole-course monitoring and management are conducted for key parts of IoT devices, device operation, working conditions, and software version upgrade etc., thus making threats found by security situation perception system was traceable and recognizable. The main contributions of this paper are as below:

- We introduce the security and privacy problems of three layers of IoT, i.e., terminal layer, network layer and application layer. Because of the diversity of terminal devices, the security problems will be brought about when the terminal devices access to the network. Furthermore, the security problem is also appeared in the network transmission, and at the remote cloud.
- In order to solve the security management of IoT terminal devices, we use the de-centralization of the blockchain and give an effective security management mechanism without the third party. In this mechanism, we will carry out security management in two situations, i.e., terminal devices and networks, terminal devices and remote cloud.

The organization of this paper is as follows. Section 2 describes security problems of IoT (including security analysis for perception layer, network layer and application layer etc.). Section 3 gives the blockchain based security architecture of IoT and corresponding analyses. Section 4 introduces open issues. Section 5 describes the conclusion of this paper.

2. Security problems of IoT

In this section, we first introduce the architecture of IoT applied to healthcare scenario. Then, we introduce the security issues for the three layers of IoT.

2.1. IoT architecture for healthcare

In this section, we first introduce the three layer for smart healthcare system, i.e., the perception layer, the network layer and the application layer. To be specific,

- The application layer is based on remote cloud which includes various specific applications of IoT (e.g., smart home, fall detection, smart healthcare [30]).

- The network layer realizes the connection between the perception layer and the application layer, which include routers, gateways and other network devices. It can connect the mobile device to the application layer, and convey the application layer instruction to the perception layer.
- The perception layer includes various sensing devices to measure the user's physical condition, such as heartbeat, blood oxygen and blood pressure. These IoT devices are connected to the remote cloud through the network layer, which enables users to transmit data to the remote cloud for analysis. After the analysis, the remote cloud feedback the results to the users.

Furthermore, when IoT is applied to smart healthcare, edge computing can be used to provide users with lower delay in medical services. This is because the edge cloud is closer to the user, usually through one hop. Furthermore, besides the smart healthcare, the IoT has been widely applied in all aspects. Thus, with the development of sensing devices, especially wearable devices and smart phones, the IoT has made many convenient applications in people's daily life. However, the IoT brings convenience as well as a lot of security and privacy problems. In the next section, we will introduce the security problems at three levels in the IoT.

2.2. Security problems of the application layer

The application layer is mainly deployed in the remote cloud, which can support a variety of services, such as smart city, smart home, smart healthcare and intelligent transportation. These diverse services need different users data. As for smart healthcare, users need to collect different data for different service types. For the detection of chronic diseases, the data that needs to be collected can be heart rate and electrocardiograph (ECG) (assuming that the chronic disease is heart disease). However, for the fall detection for old people, the data that needs to be collected may be heartbeat, blood pressure, blood oxygen, ECG. However, these collected data belong to the user's privacy data, and medical service providers need to use these data for data analysis to provide users with a reasonable service. Thus, if these data fail to be well protected, users' privacy will be leaked. Therefore, we need consider three security issue in the application layer, i.e., privacy protection of user's data, analyze encrypted data in the remote cloud and the secure computing.

When mobile devices obtain services from remote cloud, identity authentication is generally required. This is because if there is no reasonable authentication technology, it will lead to the access of malicious terminals to get services. Furthermore, when malicious users initiate DoS or DDoS attacks, it will cause legitimate users' requests for normal service requests, resulting in a decline. Although the remote cloud can take advantage of its computing and storage resources to provide identity authentication for a large number of IoT devices, it is necessary to design a reasonable identity authentication mechanism because the magnitude of the number of devices is too large. In addition, with the emergence of mobile crowdsourcing technology, users can use mobile devices to connect to the IoT, which may require a dynamic identity authentication mechanism to meet the identity authentication of a large number of dynamic mobile devices.

2.3. Security problems of the network layer

The perception layer devices can access the application layer through cellular network or WiFi. In the network layer, with the continuous development of 5G network, the network layer generally adopts the standard communication protocol. Thus, in this paper, we does not consider the security problems brought by communications.

2.4. Security problems of the perception layer

The perception layer of the IoT is connected to the application layer through the network layer. For example, in a smart healthcare scene, the user transmissions the data collected by the smart clothing to the remote cloud through cellular network or WiFi.

There are two different kinds of security threats faced by the perception layer as shown below:

- Many terminals open unsafe ports or services, and there are a large number of vulnerabilities that allow for unauthorized access. There would often be threats where hackers are able to utilize these vulnerabilities to launch wide-range DDoS attacks.
- Many terminals can be connected to the gateway through Zigbee, Bluetooth, and WIFI, but the security mechanism for these short-distance communication protocols themselves is weak, and these devices are vulnerable to hacker intrusion. Many of these terminals are lacking in a sufficiently strong login password, and these terminals are vulnerable to hacker login. There is a lack of encryption measures for communication between terminals and the platform.

3. Blockchain based IoT security system

With the increasing number of mobile devices, there are more and more devices connected to the IoT. Thus, the traditional central based security management is hard to achieve. Therefore, in this paper, we propose a de-centralization security management model based on blockchain, which realize the overall security management control without the need of the trusted third party. In this section, we first introduce the design issue. Then, we introduce the security management scheme.

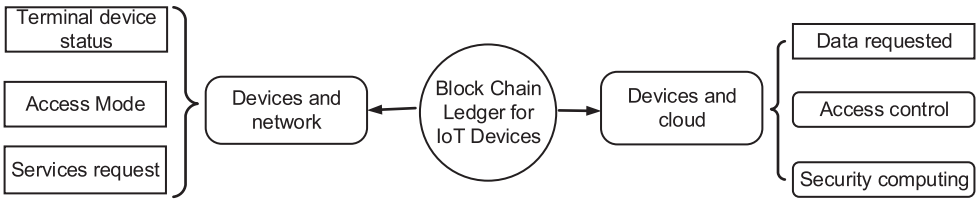

Fig. 2. Blockchain ledger structure for IoT devices.

3.1. Design issues

In view of the de-centralization of blockchain technology, a unified security managements of the IoT devices are carried out, and the change of state of various devices in the perceptual layer is grasps in time. Thus, we propose IoT security management without the participation of a trusted third party.

To realize security enforcement in perception layer of IoT, open and highly security IoT devices asset management and traceability technology are studied based on new thoughts and new methods such as blockchain. Specifically, the following research methods are adopted.

- Authentication of the IoT device. With the development of IoT, identity authentication is needed when users obtain services. However, the traditional identity authentication requires a trusted third party. Under the support of the blockchain technology, an effective identity authentication can be achieved without the third party.
- The interaction between the IoT device and the remote cloud. After the remote cloud obtains the users' data, the results of users' data processing need to be feedback. At the same time, it needs to ensure the secure transmission of the data and not be tampered with, and it needs to ensure the timely and effective data. With the support of blockchain technology, a high security management mechanism can be implemented to achieve the overall security management for IoT.

Blockchain technology means collectively maintaining a reliable database program through decentration and distrust. In this paper, we achieve the security management from the security requirements of three layers of IoT. Furthermore, we realize the overall security management of the IoT under blockchain. Fig. 2 describe a blockchain accounting structure for security management of IoT devices.

From the Fig. 2, we can see that the whole blockchain ledger structure consists of two parts, i.e., the ledger between IoT devices and network, and the ledger between IoT devices and the remote cloud. When the IoT devices connect to the network, the required ledger information includes the status of the IoT device, the access network mode of the IoT devices, and the number of requests for services, etc. When the IoT device is interacting with the remote cloud, the required ledger information includes the acquisition data of the IoT device, the identity authentication information of the IoT device, and the security sensitivity of the IoT device. By blockchain technology to record information of these IoT devices, different security policies can be implemented to achieve different security enhanced deployment. Furthermore, we can use artificial intelligence technology, machine learning, deep learning and reinforcement learning to realize the intellectualization of information processing.

3.2. Asset management for devices in the full life cycles based on blockchain

This paper puts forth a distributed storage models on IoT based on blockchain and device ledger, where related production and application of IoT devices are analyzed. The key secure links between IoT devices in the life cycle are made clear and definite. The security management model and architecture of privacy management, source tracing for parts, and software upgrade management for IoT devices in the full life cycle based on blockchain are put forth.

As shown in Fig. 3, we introduce the security management in three layer of IoT. The perception layer includes the IoT terminal devices and the IoT gateway devices. The required security management includes privacy protection, access control, authentication management, and device protection. The network layer include mobile network (e.g., 5G) and the low-power wide-area network (LPWAN). In this paper, we do not consider the analysis of the security management of the network layer. The application layer includes automatic driving, smart healthcare, industry 4.0 and smart home. The required security management includes log and auditing, privacy protection, access control, authentication management and software management.

However, with the increase of IoT devices, there are massive IoT terminals. Therefore, plenty of computing power at terminals would necessarily be consumed based on traditional blockchain technology. As for IoT, problems such as computational efficiency, privacy protection, and supervision for distributed node data management in blockchain must be solved. Therefore, the establishment of blockchain based cloud platform for IoT devices management in the full life cycle can be considered, depending on the distributed cloud computation. This platform composes of IoT devices, application software, platform providers, and union nodes interconnect to each other through the high speed network. With this blockchain platform, a more efficient cryptographic algorithm will be adopted, thus guaranteeing the requirements of low latency and high

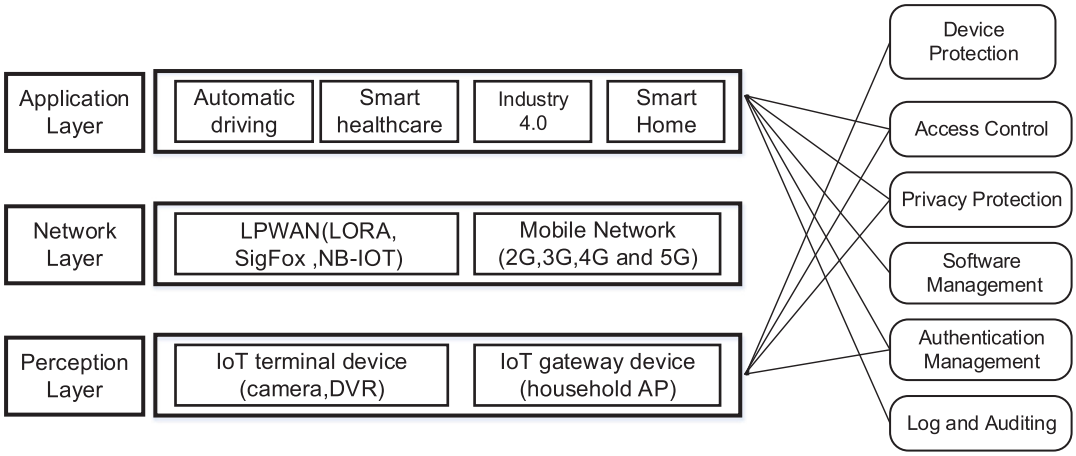

Fig. 3. Management requirements for IoT devices.

throughput in data management for IoT devices. On the other hand, in terms of connections between the IoT devices and the blockchain database, device identification-based key algorithm will be adopted to guarantee security and reliability. In the meantime, the reserved interface would be provided for regulators as far as blockchain ledgers of IoT are concerned. This would realize the necessary requirements for safety, auditing, and inspection for IoT devices.

4. Open issues

4.1. Abnormal network traffic monitoring based on machine learning

Machine learning technology have been widely applied in various fields, including rehabilitation instruments, robotic assembly tasks, autonomous vehicles etc. Using machine learning technology to detect the abnormal traffic has become a research hotspot. According to whether the network traffic of training set contains labels, we can use supervised learning or semi-supervised algorithm to implementation of abnormal traffic detection. When the data in the training set contain labels, we can use supervised algorithm (e.g., support vector machine) to detect the abnormal network traffic. When there are some data are unlabeled, we can use semi-supervised algorithm (e.g., active learning) to detect the abnormal network traffic. With the development of deep learning, we can use deep convolutional neural network (e.g., AlexNet) to detect abnormal traffic. However, when these algorithms are applied to abnormal network traffic monitoring, since most traffic is normal traffic, it will lead to waste of resource, such as the resource of storage and computation. Furthermore, these algorithms rely on labeled data, which will inevitably lead to the limitation of network abnormal traffic monitoring. Thus, it is still a challenging problem to design an efficient abnormal traffic detection for IoT.

4.2. Identity verification

With the diversification and the rapid increase of IoT device, the identity verification is still a challenging problem.

- The diversification of IoT devices brings the complexity of identity authentication. For example, the IoT device can be a static sensor (such as a deployed air quality detection sensor), or a dynamic sensor (such as a vehicle), resulting in the diversity and complexity of identity authentication of different types of IoT devices. Furthermore, with the development of cloud computing, edge computing and other technologies, it brings convenience to the IoT, and brings challenges to the data security of the IoT devices. Under these technologies, it is a challenge problem for the diversified IoT devices which can not only use cloud computing to obtain new services, but also achieve effective identity authentication, and then protect the security of data information.
- The rapid increase in the number of IoT devices leads to a large number of identity authentication tasks, which may cause the users to wait too long, therefore affecting the users' QoE. Thus, it is a worth studying for the identity authentication of mass IoT devices.

5. Conclusion

In summary, we conducted security problems analyses to three layers of IoT (i.e., application layer, network transmission layer, and perception layer). Then, we introduced blockchain based IoT security system. The design issues of this security solving methods is asset management for devices in the full life cycles based on blockchain. We study the management requirements for IoT devices, and then blockchain platform can be utilized to solve it. With the interaction between the IoT

devices and the blockchain database, a device identification-based key algorithm will be adopted to guarantee security and reliability. At last, two open problems are given, i.e., abnormal network traffic monitoring based on machine learning, and identity verification.

Acknowledgment

Dr. Pustišek Matevž would like to acknowledge the financial support from the Slovenian Research Agency (research core funding No. P2-0246). This research was supported in part by the National Natural Science Foundation of China under Grant Nos. 61772383, 61572380.

References

[1] Chen M, Hao Y. Task offloading for mobile edge computing in software defined ultra-dense network. IEEE J Sel Areas Commun 2018;36(3):1–11.
[2] Chen M, Miao Y, Hao Y, Hwang K. Narrow band internet of things. IEEE Access 2017;5:20557–77.
[3] Chen M, Tian Y, Fortino G, Zhang J, Humar I. Cognitive internet of vehicles. Comput Commun 2018;120:58–70.
[4] Lin K, Xia F, Li C, Wang D, Humar I. Emotion-aware system design for the battlefield environment. Inf Fusion 2019;47:102–10.
[5] Tian D, Zhou J, Sheng Z, Chen M, Ni Q, Leung VCM. Self-organized relay selection for cooperative transmission in vehicular ad-hoc networks. IEEE Trans Veh Technol 2017;66(10):9534–49.
[6] Qian Y, Chen M, Chen J, et al. Secure enforcement in cognitive internet of vehicles. IEEE IoT J 2018;5(2):1242–50.
[7] Kolias C, Stavrou A, Voas J, Bojanova I, Kuhn R. Learning internet-of-things security hands-on. IEEE Secur Privacy 2016;14(1):37–46.
[8] Zhang B, Liu CH, Lu J, Song Z, Ren Z, Ma J, Wang W. Privacy-preserving qoi-aware participant coordination for mobile crowdsourcing. Els Comput Networks 2016;101(4):29–41.
[9] Kim J, Holz R, Hu W, Jha S. Automated analysis of secure internet of things protocols. In: ACM proceedings of the 33rd annual computer security applications conference; 2017. p. 238–49.
[10] Usman M, Ahmed I, Aslam MI, Khan S, Shah UA. Sit: a lightweight encryption algorithm for secure internet of things. 2017. arXiv:1704.0868.
[11] Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Veh Commun 2014;1(2):53–66.
[12] Zhang K, Ni J, Yang K, Liang X, Ren J, Shen X. Security and privacy in smart city applications: challenges and solutions. IEEE Commun Mag 2017;55(1):122–9.
[13] Chen J, He K, Yuan Q, Xue G, Du R, Wang L. Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks. IEEE Transactions on Mobile Computing 2017;16(6):1530–43.
[14] Lansiti M, Lakhani KR. The truth about blockchain. Harv Bus Rev 2017;95(1):119–27.
[15] Dorri A, kanhere S, Jurdak R. Blockchain in internet of things: challenges and solutions. 2016. arXiv:1608.05187.
[16] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access 2016;4:2292–303.
[17] Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: High performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), 2016 IEEE 18th international conference on. IEEE; 2016. p. 1392–3.
[18] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for iot security and privacy: the case study of a smart home. In: Pervasive computing and communications workshops (PerCom workshops), 2017 IEEE international conference on. IEEE; 2017. p. 618–23.
[19] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for iot. In: Proceedings of the second international conference on internet-of-things design and implementation. ACM; 2017. p. 173–8.
[20] Zhang Y, Chen M, et al. SOVCAN: safety-oriented vehicular controller area network. IEEE Commun 2017;55(8):94–9.
[21] Zhang Y, Wen J. The iot electric business model: using blockchain technology for the internet of things. Peer-to-Peer Network Appl 2017;10(4):983–94.
[22] Liao CF, Bao SW, Cheng CJ, Chen K. On design issues and architectural styles for blockchain-driven iot services. In: 2017 IEEE international conference on consumer electronics-Taiwan (IEEE ICCE-TW); 2017. p. 351–2.
[23] Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. In: 2017 19th international conference on advanced communication technology (IEEE ICACT 2017); 2017. p. 464–7.
[24] Ghuli P, Kumar UP, Shettar R. A review on blockchain application for decentralized decision of ownership of IoT devices. Adv Comput Sci Technol 2017;10(8):2449–56.
[25] Kim H, Laskowski M. Towards an ontology-driven blockchain design for supply chain provenance. Int Syst Account, Finance Manag 2018;25(1):18–27.
[26] Chen M, Hao Y, Hu L, Huang K, Lau V. Green and mobility-aware caching in 5g networks. IEEE Trans Wireless Commun 2017;16(12):8347–61.
[27] Chen M, Hao Y, Qiu M, Song J, Wu D, Humar I. Mobility-aware caching and computation offloading in 5g ultradense cellular networks. Sensors 2016;16(7):974–87.
[28] Chen M, Qian Y, Hao Y, Li Y, Song J. Data-driven computing and caching in 5g networks: architecture and delay analysis. IEEE Wireless Commun 2018;25(1):70–5.
[29] Ge X, Li Z, Li S. 5G software defined vehicular networks. IEEE Commun Mag 2017;55(7):87–93.
[30] Chen M, Yang J, Zhou J, Hao Y, Zhang J, Youn C. 5G-smart diabetes: towards personalized diabetes diagnosis with healthcare big data clouds. IEEE Commun 2018;56(4):16–23.

Yongfeng Qian is an associate professor in China University of Geosciences, Wuhan, China. She received the Ph.D degree in School of Computer Science and Technology at Huazhong University of Science and Technology (HUST) in 2018. Her research interests include software defined network, security and privacy, cloud computing and the Internet of Things.

Yingying Jiang received the B.Sc. degree from School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan, China in 2017. Currently, she is a Ph.D candidate in School of Computer Science and Technology, HUST since 2017. Her research interests include healthcare big data, cognitive learning, etc.

Jing Chen received the Ph.D. degree in computer science from Huazhong University of Science and Technology, Wuhan. He worked as an associate professor from 2010. His research interests are in the areas of network security, cloud security. He is the Chief Investigator of several projects in network and system security, funded by the National Natural Science Foundation of China (NSFC).

Yu Zhang received the B.Eng. degree from School of Computer Science and Technology, Chongqing University, China in 2017. Currently, she is a Master candidate in School of Computer Science and Technology, HUST since 2017. Her research interests include emotional monitoring, cognitive learning.

Jeungeun Song is with Department of Electrical and Computer Engineering, The University of British Columbia, Canada. She received the Ph.D degree in School of Computer Science and Technology at Huazhong University of Science and Technology (HUST) in 2018. Her research focuses on Internet of Things, Mobile Cloud, Body Area Networks, Emotion-aware Computing, Healthcare Big Data, Cyber Physical Systems, and Robotics.

Ming Zhou (mingzhou.hust@gmail.com) is lecturer in the School of Energy and Power Engineering at Huazhong University of Science and Technology (HUST). He is general manager in insititue of new energy at Wuhan. He received his Ph.D. degree in control theory and control engineering from the Department of Control Science and Engineering at HUST in 2011. His research interests include network communication, intelligent control, detection technology, and automatic equipment.

Matevž Pustišek is a Senior Lecturer at the Faculty of Electrical Engineering, University of Ljubljana, Slovenia. His research is focused on Internet services and applications, including mobile, Web, and IoT. A special interest is oriented towards IoT architectures and security aspects. Recently additional focus is set on use of blockchain technologies in IoT.