DOI: 10.3969/j.issn.1673-5188.2017.S2.008
http://kns.cnki.net/kcms/detail/34.1294.TN.20180102.1545.004.html, published online January 2, 2018

Security Enhanced Internet of Vehicles with Cloud-Fog-Dew Computing

MENG Ziqian[1], GUAN Zhi[2,3], WU Zhengang[4], LI Anran[1], and CHEN Zhong[1]

(1. School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China;
2. National Engineering Research Center for Software Engineering, Peking University, Beijing 100871, China;
3. Laboratory of High Confidence Software Technologies, Peking University, Beijing 100871, China;
4. The Third Research Institute of China Electronics Technology Group Corporation, Beijing 100015, China)

Abstract

The Internet of Vehicles (IoV) is becoming an essential factor in the development of smart transportation and smart city projects. The IoV technology consists of the concepts of fog computing and dew computing, which involve on-board units and road side units in the edge network, as well as the concept of cloud computing, which involves the data center that provides service. The security issues are always an important concern in the design of IoV architecture. To achieve a secure IoV architecture, some security measures are necessary for the cloud computing and fog computing associated with the vehicular network. In this paper, we summarize some research works on the security schemes in the vehicular network and cloud-fog-dew computing platforms which the IoV depends on.

Keywords

cloud computing; dew computing; IoV; privacy; security

1 Introduction

The Internet of Vehicles (IoV) is believed to become the first real life implementation of the Internet of Things (IoT). The IoV plays an essential role in building smart cities and the future of transportation. Generally, the IoV technology consists of several concepts. The on-board units (OBU), associated with a wide range of sensors in vehicles, provides all kinds of data needed for applications and service. Due to the limited computational resources in vehicles' on-board devices, the power of cloud computing is needed for compute-intensive services. The road side units (RSU), which communicate with OBU through wireless network, provide connectivity between the vehicle and data center. The data center in the IoV architecture provides the computational resources needed for location-based services and other services required by vehicles. In the IoV architecture, the OBU and RSU are the components of the edge network between the backbone network and vehicles, which fit perfectly into the concept of fog computing. The OBU and RSU, as the fog nodes in fog computing, can process most of the vehicle data yet the power of cloud computing is still required for the compute-intensive works.

On the other hand, security issues are always an important concern in the IoV technology. Traditional security measures, such as authentication, digital signature and encryption, can provide vehicular network with protection to some extent. However, due to the frequent handover of network connection resulted from fast movement of vehicles, those traditional security measures do not meet the special security requirements of vehicular network. The security measures are extremely difficult to be deployed on the OBU and RSU due to their limited computational power, which makes these devices vulnerable to attacks. The privacy-preserving is also an issue that need to be considered in the design of IoV architecture.

This research work is supported by National Natural Science Foundation of China under Grant No. 61672060.

2 Background

2.1 Internet of Vehicles

The IoV consists of vehicles, sensors and actuators, roadside infrastructures and other devices. The seamless integration of these components is one of the biggest challenges of the IoV to improve the traffic condition and safety levels. To solve this problem, many solutions have been proposed to design a layered IoV system with different focuses.

A three-layer architecture has been proposed based on the interaction of different technologies in the IoV environment [1]. The bottom layer gathers all the environmental data and detects specific events of interest such as driving patterns, environmental conditions and vehicle situations with all the sensors in the vehicles. The middle layer (communication layer) aims at providing a common communication platform for different wireless nodes. The top layer (control layer or functional layer) is responsible for storage, analysis processing and deci-

sion making in different risk situations.

To make the vehicles connect the Internet and get kinds of services for drivers, a four-layer IoV architecture has been proposed [2], which enables the Vehicle-to-Business (V2B) communication. The four layers are named as the end-point layer, infrastructure layer, operation layer and service layer.

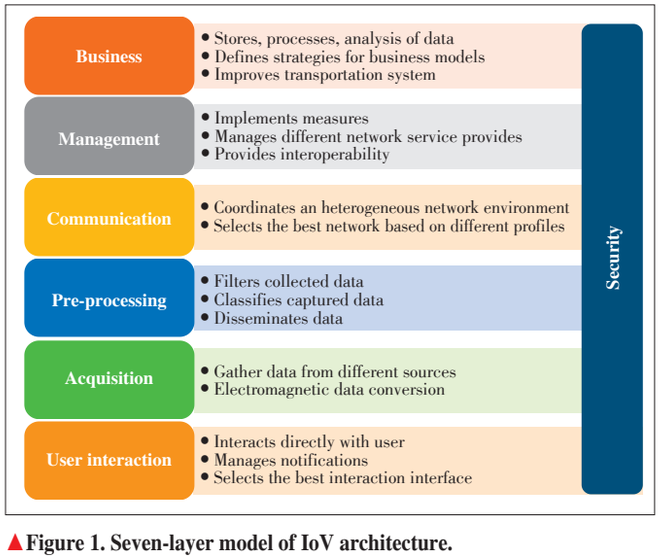
A seven-layered model for the IoV has further been proposed, which supports the functionalities, interactions, representations and information exchanges among all the devices in the IoV system [3]. This architecture aims at providing a seamless integration for inter-device communication in the IoV ecosystem and takes care of some security problems. **Fig. 1** shows this seven-layer model.

2.2 Cloud Computing and Fog Computing

Cloud computing was first introduced by Professor Ramnath Chellappa in 1997 [4]. It changes the boundaries of the computing from technical limits to economic rationale. In the concept of cloud computing, users can get a single and homogenous service anywhere from the cloud without taking care of the complexity and heterogeneity.

Fog computing, defined as a new computing paradigm, was first introduced by CISCO Systems Inc. in 2011 [5]. It provides data, computation, storage and application services from closer devices to clients or end-users, rather than sending data to remote servers in the cloud. The use of fog computing can improve the efficiency of data processing in network and enhance the network security [6].

In the IoV system, a vehicle needs to connect to surrounding vehicles and devices and communicates with them. This requirement just coincides with the framework of fog computing thus we can build fog computing service for the IoV system. In this way, the bandwidth and energy consumption will get a significant improvement, without sending the massive data generated by different kinds of IoV devices to cloud computing service or a centralized networking infrastructure [7].



▲Figure 1. Seven-layer model of IoV architecture.

2.3 Standards for Internet of Vehicles

In the IoV, there are different technologies, services and standards that need to be integrated for them to work in harmony [8]. At the same time, different types of participants in the IoV need appropriately interconnected with each other. To achieve this goal, many standards need to be set for the IoV framework.

The IoV is a key component of the IoT. Therefore, almost every application-layer protocols in the IoT can be implemented in the IoV. **Fig. 2** shows the primary protocols for the IoV [9].

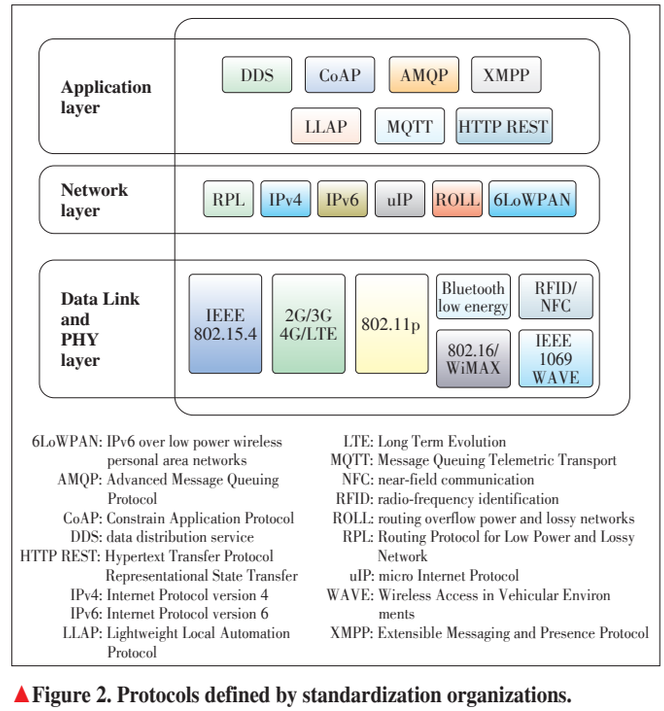
3 Security in Internet of Vehicles

3.1 Security Requirement in Internet of Vehicles

With the heterogeneity and the large number of vehicles, data security in the IoV is becoming a challenging problem. **Table 1** shows the most important security requirements for the IoV [10].

3.2 Security Solutions to Internet of Vehicles

Traditional security measures, such as authentication, digital signature and encryption, can provide vehicular network with protection to some extent. However due to the frequent handover of network connection resulted from fast movement of the vehicles, the traditional security measures fail to meet the special security requirements of the IoV. The connections in vehicular network are short, temporary and involving lots of



▲Figure 2. Protocols defined by standardization organizations.

▼Table 1. Security requirements of the IoV

Security requirement	Description
Data authentication	When data is transferred, the identities of vehicles must be verified
Data integrity	Transmitted and received data must be checked to ensure that data is delivered correctly
Data confidentiality	Data must be protected to ensure secret data transmission occurs between different vehicles participating in the IoV
Access control	In the IoV, vehicles should only access available services that they are entitled to
Data non-repudiation	A vehicle cannot deny the authenticity of another vehicle
Availability	The communication between different vehicles should be ensured
Anti-jamming	Mechanisms should be built to prevent malicious vehicles from sending interfering messages to interrupt the normal communication between vehicles

fast handover operations. Some solutions have been proposed to solve the security issues in the IoV.

There are two types of identity attacks in vehicular network. The first one is Sybil attacks, which forges fake identities and pretends to be multiple users in peer-to-peer network. Sybil attacks are mostly like to happen in the network where there are no methods, such as digital signature and certificate authority (CA), to verify users' identities. For example, a malicious car can create a large number of fake identities to trick navigation software and make it believe that the traffic is heavy, in order to own the road exclusively. The other type is identity theft. The identity of a legit car can be stolen by malicious users and used in illegal activities. Multiple malicious cars can conduct misbehaviors in several places at the same time using the same identity, which would cause lots of trouble in developing security countermeasures.

Identity attacks are often conducted through a legit identity, which is beyond the protection from passwords or other identity authentication methods. The studies on identity attacks in vehicular network mainly focus on detection, instead of prevention, of the identity theft.

Some studies are based on the fact that a vehicle with legit identity can appear at only one location at any given time. Thus, the identity attack and theft can be detected by binding the vehicle's identity with its location. Some researchers have proposed identity theft detection methods based on vehicle's motion trajectories [11]–[13]. The main idea of the detection methods is comparing the location data from road-side units, such as the driving routes of a group of vehicles within short distance or the distance between two vehicles with the same identity.

On the other hand, vehicles' sensitive location and privacy data can be stolen or leaked by road-side units and location-based services. Data privacy in vehicular network has three aspects: the privacy of drivers' (users') identity, the privacy of vehicles' identity and the privacy of vehicles' location. The privacy of vehicles' location is the hardest and most important issue among these three aspects since a vehicle needs to provide its location to access services. There has been much research focused on the privacy-preserving methods. The basic idea of preserving vehicles' location is eliminating the mapping between the vehicle's identity and the identity used in its communication with LBS and RSU [14]. There are two kinds of proposed schemes to hide the vehicle's identity. The first one uses pseudonyms in communications. Pseudonyms are the temporary identities that are assigned by a vehicle itself or CA. A vehicle is allowed to have multiple pseudonyms to use in different communications and the pseudonyms can be changed in the assigned area called mix zones. Mix zones are the special areas where vehicles' locations are not detectable. Multiple vehicles may traverse through the mix zone and change their pseudonyms at the same time, which mixes the mapping between the pseudonym and the vehicle and makes it difficult to match the identity and the vehicle. The concept of pseudonyms and mix-zones were first proposed by Beresford [15] based on the assumption that RSU and LSB providers were hostile. The shortage of pseudonym-based schemes is due to the involvement of the complicated pseudonym management caused by the large number of pseudonyms and encryption keys required in the schemes. The second kind of privacy-preserving schemes uses group signature [16]–[19]. A certificate is assigned to a group of vehicles and every member in this group can sign the message with the same public key. In this way, adversaries cannot know the identity of the real signer of the message while the group leader has the ability to reveal the identity of the actual message signer for audit purpose. The group signature based schemes are usually time consuming because of the extra operations needed in the encryption and decryption processes of the group signature mechanism.

3.3 IoV Security in Fog Computing

All the computing components in the IoV, such as on-board units, road side units, and vehicles themselves, are fit perfectly into the concept of fog computing as these units can provide connectivity and interaction between vehicles and cloud platforms. All the computational units can be considered as fog nodes at the edge networks. However, due to the limited computational resources of the road side units, security mechanism is very hard to deploy in the fog nodes, which may bring serious security issues to the IoV.

Besides the privacy problem of the vehicles, there are several other security issues related to the vehicular network and fog computing. The location-based services in the IoV highly depend to the precise location of the vehicle. Therefore, the location verification and detection of location spoofing is a crucial issue to the quality of location-based service. The model of trust relationship is also a serious security issue of the vehicular network since every vehicle and road side unit can be malicious. The fast movement of vehicles and traffic jams in rush hours can cause some serious scalability issues as well. The fog computing platform, along with fog nodes, should provide

different security levels for different vehicles. Obviously, a taxi should not have the same protection of "Army One" of the president.

Since the fog computing and IoV are relatively new diagrams, the security issues of the IoV in fog computing scenario has not attracted much research. However, Yan et al. [20] proposed a method of partitioning the city or traffic area into a number of grids. Each grid is managed by one virtual machine or a set of virtual machines in the cloud platform, thus the whole city can be mapped to the cloud. Each virtual machine is associated with a large number of road side units. When a particular grid is congested or more strict regulations are needed, the virtual machine can request more computing and storage resource from the cloud platform to enforce more security protocols. Furthermore, each corresponding virtual machine can be individually configured and optimized for smart parking and congestion control.

3.4 Security Enhanced IoV in Cloud Computing, Fog Computing and Dew Computing

Modern motor vehicles are complicated electromechanical integrated devices. With the development of the IoV, the vehicle has gradually become an intelligent terminal with rich functions beyond smartphones. First, the vehicle itself integrates more and more sensors, controllers and processors to achieve more advanced driving control functions, including auxiliary driving, automatic driving and other functions. Second, the vehicle will be more convenient to access the IoT and interact with remote data centers or service providers and gradually realize the functions of intelligent transportation. Hubaux et al. [21], first studied security and privacy problems for the intelligent cars connected to the IoV from the intelligent terminal point of view in 2004. In addition to the security of information systems and their networks, the security of connected vehicles is also concerned about the following issues:

- Anomaly detection: Find and locate illegal vehicles and fake vehicle identification cards
- Risk assessment: information security risk assessment for intelligent motor vehicle and information systems in IoV
- Identification: the vehicle identification under normal circumstances mainly depends on license plates and RFID, while the vehicle identification under abnormal conditions where the vehicle identity information cannot be recognized is implemented by a variety of other features.
- Privacy protection: protect the identity of motor vehicle owners, moving trajectory and other sensitive data.
- Safe driving: automatic driving, auxiliary driving and other technologies are to improve the safety and ease of use of the car itself.

Cloud computing, fog computing, and dew computing are the distributed and intelligent computing models that are gradually enhanced [22]. Car networking is a huge and complex information system, involving the relationship between the massive complex entities in the real world and a variety of roles such as all types of motor vehicles, various types of services, all kinds of regulatory agencies, and road network maps. By virtue of the advantages of cloud, fog and dew computing models, the vehicle ad hoc network (VANET), IoV and smart IoV can be gradually constructed, and accordingly integrated intelligent traffic will be realized. Because of the practical need of vehicle networking, cloud computing, fog computing and dew computing are gradually applied to the vehicle network, and the resulting new security issues have been studied:

Bhatia et al. [23] studied security issues in mobile cloud computing. Cloud computing provides a centralized data processing and computing platform in the vehicle network. The related security problems are mainly caused by the outsourcing of data storage and computing, including data security and sensitive information leakage.

Alrawais et al. [24] studied the security and privacy issues of fog computing in the IoT. Different from cloud computing, fog computing does not totally rely on the computing resource in the remote data center hence the data generated by IoT devices can be stored in the nearby fog nodes, which alleviates the risk of data and calculation of complete outsourcing. However, the vulnerability of the fog node itself has caused concern.

Dew computing can support smart objects following cloud computing [25], which is more suitable for distributed intelligent IoV computing platform. The intelligent computing usually involves high complexity of scientific computing tasks, such as image recognition, path planning, automatic driving, driver assistance, voice recognition and other high level intelligence functions in large information systems, to simplify the deployment and service approaches. The artificial intelligence algorithms can control the vehicle and is heavily dependent on input data, so these algorithms may mislead the vehicle through the operation of the disastrous consequences of original input data errors, implied new security problems.

4 Conclusions

This paper discussed different attacks to the IoV, as well as some countermeasures including identity verification and privacy - preserving methods. The situation in which cloud, fog and dew computing diagrams are being combined with IoV technology was also presented. We believe that the concepts of cloud, fog and dew computing will play important roles in the future development of IoV technology as they can provide a whole new secure architecture and computing platform for the vehicular network. However, there are some security issues need to be addressed to achieve the successful integration of IoV technology and the concepts of cloud, fog and dew computing. There are few studies focused on the secure connection between the data center and edge vehicular network, which has a potential to be eavesdropped for stealing sensitive data. The combination of heterogeneous networks also needs to be ad-

dressed with effective security protocols to protect vulnerable devices in the edge network. In conclusion, with the power of cloud, fog and dew computing, the IoV technology has the potential to shape the future of our transportation. At the meantime, the future research work should focus on the security issues that rise among the integration of the IoV and cloud, fog and dew computing systems as the security is always an essential concern in the design of vehicular network architecture.

References

[1] K. Golestan, R. Soua, F. Karray, and M. S. Kamel, "Situation awareness within the context of connected cars: A comprehensive review and recent trends," *Information Fusion*, vol. 29, pp. 68–83, May 2016. doi: 10.1016/j.inffus.2015.08.001.
[2] F. Bonomi, "The smart and connected vehicle and the internet of things," Invited Talk, Workshop on Synchronization in Telecommunication Systems, 2013.
[3] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, Apr. 2017. doi: 10.1109/JIOT.2017.2690902.
[4] R. Chellappa, "Intermediaries in cloud-computing: a new computing paradigm," in *INFORMS Annual Meeting*, Dallas, USA, Oct. 1997.
[5] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proc. First Edition of MCC workshop on Mobile cloud computing*, Helsinki, Finland, 2012, pp. 13–16. doi: 10.1145/2342509.2342513.
[6] K. Shenoy, P. Bhokare, and U. Pai, "Fog computing future of cloud computing," *International Journal of Science and Research*, vol. 4, no. 6, pp. 55–56, Jun. 2015.
[7] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5 pp. 637–646, Oct. 2016. doi: 10.1109/JIOT.2016.2579198.
[8] J. Cheng, J. Cheng, M. Zhou, et al., "Routing in internet of vehicles: a review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015. doi: 10.1109/TITS.2015.2423667.
[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. doi: 10.1109/COMST.2015.2444095.
[10] B. Mokhtar, and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015. doi: 10.1016/j.aej.2015.07.011.
[11] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban vanets," in *29th IEEE International Conference on Distributed Computing Systems Workshops*, Montreal, Canada, 2009. doi: 10.1109/ICDCSW.2009.48.
[12] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *IEEE Military Communications Conference*, Boston, USA, 2009. doi: 10.1109/MILCOM.2009.5379844.
[13] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012. doi: 10.1109/TPDS.2011.263.
[14] Z. Zhang, et al., "Study on location privacy protection technology of VANET," *Journal on Communications*, vol. 33, no. 8, pp. 180–189, 2012.
[15] A. R. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," in *Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, Orlando, USA, 2004. doi: 10.1109/PERCOMW.2004.1276918.
[16] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Computers & Electrical Engineering*, vol. 38, no. 3, pp. 573–581, May 2012. doi: 10.1016/j.compeleceng.2011.11.009.
[17] J. Chen, M. S. I. Mamun, and A. Miyaji, "An efficient batch verification system and its effect in a real time VANET environment," *Security and Communication Networks*, vol. 8, no. 2, pp. 298–310, 2015. doi: 10.1002/sec.980.
[18] Lin, Xiaodong, et al. "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007. doi: 10.1109/TVT.2007.906878.
[19] J. Zhang and Y. Xu, "Privacy- preserving authentication protocols with efficient verification in VANETs," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 3676–3692, 2014. doi: 10.1002/dac.2566.
[20] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 284–294, Mar. 2013. doi: 10.1109/TITS.2012.2211870.
[21] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, May-Jun. 2004. doi: 10.1109/MSP.2004.26.
[22] K. Skala, D. Davidovic, E. Afgan, I. Sovic, and Z. Sojat, "Scalable distributed computing hierarchy: cloud, fog and dew computing," *Open Journal of Cloud Computing* , vol. 2, no. 1, pp. 16–24, 2015.
[23] T. Bhatia and A. K. Verma, "Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues," *The Journal of Supercomputing*, vol. 73, no. 6, pp. 2558–2631, Jun. 2017. doi:10.1007/s11227-016-1945-y.
[24] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, Mar.-Apr. 2017. doi: 10.1109/MIC.2017.37.
[25] A. Rindos and Y. Wang. "Dew computing: the complementary piece of cloud computing," *IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)*, Atlanta, USA, 2016. doi: 10.1109/BDCloud-SocialCom-SustainCom.2016.14.

Manuscript received: 2017-06-17

Biographies

MENG Ziqian (markmzq@pku.edu.cn) is a Ph.D. candidate of Ministry of Education (MoE) Key Laboratory of Network and Software Security Assurance of Peking University, China. He received his bachelor degree in computer science from Peking University in 2013. He visited Carnegie Mellon University, USA as a visiting scholar for one year in 2016. His current research interests include future Internet architecture, network security, mobility, congestion control and the IoV.

GUAN Zhi (guan@pku.edu.cn) received his Ph.D. degree in computer science from Peking University, China in 2009. He is a faculty member of MoE Key Laboratory of Network and Software Security Assurance of Peking University since 2009. He is an associate professor and his current research interests include cryptography engineering, crypto-currency and cloud security. He gives lectures "Introduction to Information Security" and "Recent Advances in Information Technology" to undergraduates and "Network and Information Security" to master students. He will give the lecture "Practical Applications of Cryptography" to master students of Mannheim University.

WU Zhengang (markzgwu@163.com) received his Bachelor's degree in engineering from Beijing Institute of Technology, China in 2003. He received his Master's degree in software engineering and Ph.D. in computer software and theory from Peking University, China in 2015 and 2006 respectively. He is a research engineer at The Third Research Institute of China Electronics Technology Group Corporation (CETC), focusing on computer science and technology. His research interests include mobile Internet security, software engineering and enterprise information system. He has published 7 academic papers as the first author, on security and privacy protection of the mobile Internet.

LI Anran (lianran@pku.edu.cn) obtained B.S. from Beijing Normal University, China and is a graduate student of Information Security Lab., Peking University, China in the third year. His research interests include information security and blockchain. Over the first two years in Information Security Lab., his research focused on cryptology and blockchain technology, and have applied a patent on managing bitcoin address efficient.

CHEN Zhong (zhongchen@pku.edu.cn) received the B.S., M.S. and Ph.D. degrees in computer science from Peking University, China. He is the director of MoE Key Laboratory of Network and Software Security Assurance of Peking University. His research interests include software engineering, information security and future Internet architecture. He is also a member of the IEEE, senior member of China Institute of Electronics, deputy director of China Software Industry Association, fellow and co-chair of professional committee of Information Security and Privacy of China Computer Federation.