Hindawi
Security and Communication Networks
Volume 2018, Article ID 3680851, 7 pages
https://doi.org/10.1155/2018/3680851

Research Article

A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things

Chen Wang[1], **Jian Shen**[2,3], **Qi Liu**[1], **Yongjun Ren**[1] and **Tong Li**[4]

[1] *School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2] *Jiangsu Engineering Center of Network Monitoring, Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[3] *State Key Laboratory of Information Security, Institute of Information Engineering, China*
[4] *College of Computer and Control Engineering, Nankai University, Tianjin 300071, China*

Correspondence should be addressed to Tong Li; litongziyi@mail.nankai.edu.cn

Received 29 March 2018; Accepted 15 April 2018; Published 17 May 2018

Academic Editor: Laurence T. Yang

Internet of Things (IoT) is a research field that has been continuously developed and innovated in recent years and is also an important driving force for the improvement of people's life in the future. There are lots of scenarios in IoT where we need to collaborate through devices to complete tasks; that is, a device sends data to other devices, and other devices operate on the aid of the data. These transmitted data are often users' privacy data, such as medical data and grid data. We propose an instant encrypted transmission based security scheme for such scenarios in IoT. The analysis in this paper indicates that our scheme can guarantee the security of users' data while ensuring rapid transmission and acquisition of instant IoT data.

1. Introduction

The Internet of Things (IoT) is a novel network connecting items, such as users, vehicles, and home devices, through electronic tags, sensors, actuators, and interactive software. IoT ensures the connection and communication between the objects by digital means. Scenarios such as intelligent vehicle system and smart home system can be more convenient, comprehensive, and intelligent with the assistance of IoT technology [1, 2].

IoT involves collaboration between different levels and various fields of technologies, including hardware, image and video processing, data mining, remote control, data security, and privacy protection [3–7]. Experts and scholars have carried out many research achievements on IoT related technologies and their practical applications from many aspects. Note that IoT may involve users' sensitive information, such as behavior habits, identity information, and medical data. Therefore, the data security protection of IoT is particularly important. Various security protocols specially designed for IoT have been proposed to achieve secure communication, ensure data integrity, and secure data sharing in IoT. However, the research of efficient instant secure transmission scheme is still in the exploratory stage. Instant encrypted transmission is a technology that consumes few resources and realizes information security in a short period of time. This kind of technology can be used in many scenes, especially in emergence situations, such as accidents, fires. To better illustrate this demand, the situation when a smart home equipped with IoT is on fire is described in detail [8–14].

A smart home may be equipped with smoke detection and analysis device, temperature monitor, image and video recognition and analysis device, gas valve control device, window control device, and fire extinguishing device [15]. Firstly, it is necessary to find danger at the first time of the fire by means of smoke alarm, temperature monitoring, and video surveillance. Secondly, when the house is on fire, the devices need to collaborate to find out the material for the fire and the factors that may further spread the fire. Finally, the

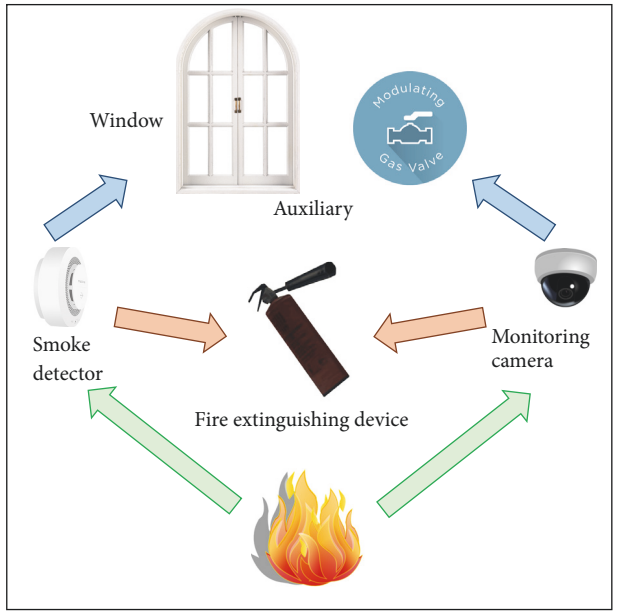

Figure 1: The illustration of IoT-auxiliary fire extinguishing.

system can decide the state of windows and valves by judging the composition of fire objects and fire situation and control the fire by fire extinguishers and other actuators. Figure 1 is an illustration of how a smart home equipped with IoT is on guard when the house fires.

Motivation of This Paper. There are some special scenarios in IoT that require the implementation of instant encrypted transmission between two entities. The car accident in the intelligent vehicle system and the fire in the smart home system require rapid transmission of sensitive information. Especially when there is a fire in a home, the camera data obtained from the home and the control instructions for valves, extinguishing devices, and other actuators are very important sensitive data. The security scheme for transmitting these information is not only to ensure the security of data transmission, but also to ensure the timeliness of data. Therefore, it is particularly important to propose a novel security scheme based on instant encrypted transmission for the application of IoT in emergency.

1.1. Our Contributions

(i) *A special and practical application scenario is discussed:* for now, there are no research and discussion on IoT-based smart home fire emergency schemes. Although this scenario rarely occurs, it has important research significance because it is likely to cause personal safety and property damage. In addition, the study of this scenario will be further extended to the design of secure transmission schemes for similar scenarios such as car accidents.

(ii) *An instant encrypted transmission method is designed:* we have tailored a method for IoT-based smart home environments. The method is mainly aimed at early warning and rescue of fire in the smart home networks. At present, few solutions have been proposed for the transmission of private data under this scenario.

(iii) *A security scheme that takes very little time is proposed:* the scheme proposed in this paper can help to solve the emergence response issue in the smart home environment. It also can be applied to other scenarios that have strict time requirements for the transmission of encrypted data.

1.2. Related Works. Cloud computing technology [16–18] is commonly utilized to solve various problems for IoT, and also brings many security challenges. Many existing security schemes can be applied into IoT with some improvements [19–23]. Sajid et al. [24] present the security challenges of cloud-assisted IoT-based supervisory control and data acquisition systems and also provide the existing best practices and recommendations for improving and maintaining the system security.

In addition, IoT is one of the important technologies for smart grid systems. Chin et al. [25] consider that energy big data needs to be stored thoughtfully and security and blackout warnings should be presented in the first time. So they survey the security threats of energy big data in IoT-based smart grid systems.

Besides, most IoT devices require location services. Location data often contains private information. Chen et al. [26] investigate robustness, security, and privacy issues in location-based services for IoT. Cryptographic solutions for security and privacy of location information and localization and LBSs in IoT are listed and compared to each other in their paper.

Saxena et al. [27] present an authentication protocol for IoT-enabled LTE network. They propose symmetric key algorithms for the efficiency. They claim that the communication overhead of their protocol is also reduced.

Aman et al. [28] propose a physical unclonable function based lightweight mutual authentication protocol for IoT systems. The adaptability of this new technology in IoT remains to be further explored.

Li et al. [29] present a novel key encryption scheme to establish a lightweight mutual authentication protocol for smart city applications. They claim that their protocol has made a trade-off between the efficiency and communication cost without sacrificing the security.

Sciancalepore et al. [30] consider that the significant airtime consumption required to exchange multiple messages and certificates and perform authentication and key agreement which are the most important issues for IoT. So they propose a public key authentication and key agreement scheme for IoT devices with minimal airtime consumption.

Furthermore, IoT is also an important industrial pillar technology in the field of health care in the future. A novel authentication scheme for medicine anticounterfeiting systems with IoT is presented by Wazid et al. [31]. The novel scheme is utilized for checking the authenticity of pharmaceutical products.

Parne et al. [32] propose a novel AKA protocol based on security enhanced group for M2M communication in a LTE/LTE-A network utilizing IoT technology. They claim that their novel protocol has better performance in overheads and fulfills security requirements of M2M communication.

Although these solutions proposed and solved many existing IoT security problems, none of them proposed a secure transmission scheme for IoT networks in a smart home environment. Simultaneously, instant encrypted transmissions in emergence situations have also not been considered.

1.3. Organization. The remainder of this paper is organized as follows. Section 2 presents some preliminaries of this paper. Section 3 shows the security models of the novel scheme. Section 4 presents the proposed scheme in detail. Section 5 states the security analysis of the proposed scheme. Section 6 presents the performance analysis of the scheme. Finally, the conclusions are drawn in Section 7.

2. Preliminaries

In this section, some necessary preliminaries utilized in this paper are listed, including bilinear pairing, system model, and scheme components.

2.1. Bilinear Pairing. $\mathbb{G}_1$ and $\mathbb{G}_2$ are two groups of prime order q. $\mathbb{G}_1$ is an additive group, and $\mathbb{G}_2$ is a multiplicative group. Set e as a mapping on $(\mathbb{G}_1, \mathbb{G}_2)$: $\mathbb{G}_1^2 \to \mathbb{G}_2$. The cryptographic bilinear map e satisfies the following properties.

Bilinearity. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in Z_q^*$. This can be expressed in the following manner. For $P, Q, R \in \mathbb{G}_1$, $e(P + Q, R) = e(P, R)e(Q, R)$.

Nondegeneracy. If P is a generator of $\mathbb{G}_1$, then $e(P, P)$ is a generator of $\mathbb{G}_2$. In other words, $e(P, P) \neq 1$.

Computability. e is efficiently computable.

2.2. System Model. The system model of our novel scheme is composed of three roles: KGC, the sender, and the receiver. The meanings of the three roles are introduced as follows.

KGC. KGC is an abbreviation of key generation center. The KGC is responsible for generating important parameters for registering each node in the system, including processing node identity information, generating system public and private keys, and generating a unique identity-based private key for each node.

Sender. The sender can be a sensor, such as an infrared device, a temperature-sensitive device and a pressure-sensitive device, or a detector, such as a smoke detector. For instance, in a fire scenario, the sender may need to collect various fire-related data in the room and encrypt the data for transmission to other nodes.

Receiver. The receiver may be various types of actuators such as fire extinguishing devices, smart windows, and gas valves. The receiver needs to receive the fire-related information sent by the sender and decrypt the relevant information through certain calculations. After real-time data is acquired, corresponding operations are performed according to different situations.

2.3. Scheme Components. This subsection mainly introduces the input and output parameters of the algorithms involved in this scheme.

Registration (ID, 1^k). This phase is run by KGC. The input of this phase is the ID number of the node. The output is an ID-related parameter q, a public key P_{pub}, and an ID-related private key s.

Detection (q_1, q_2, s_1, m). The sender performs this phase. Let q_1, q_2, the secret key s_1, and the fire message m be the input. The output is encrypted message M, certification message R, and public key for this round X.

Implementation(q_1, q_2, s_2, M, R, X). This phase is run by the receiver. The receiver takes q_1, q_2, his secret key s_2, the encrypted message M, the certification parameter R, and X as its input. The output is the decrypted message m.

The above three main algorithms constitute the main part of our new scheme.

3. Security Model

In this section, we introduce three security models for our proposed scheme.

3.1. A Forged Sender. A forged sender may be a sensor node in IoT whose identity information has been stolen. The forged sender can broadcast a wrong message using the identity of the real one. This kind of wrong information can lead to extremely serious consequences. For example, when a house is on fire, an attacker can broadcast some normal monitoring data, which makes the whole system unable to monitor the fire for the first time. In addition, when a house is in a normal state, a forged node will send an "on fire" signal to the whole system, which will also cause irreparable damage to the user.

3.2. Man-in-the-Middle (MITM) Attack. A man-in-the-middle (MITM) attack refers to the situation that a man-in-the-middle intercepts the information sent by the sender and sends the information to the receiver after some malevolent tampering. This can also cause the spread of false information and serious consequences.

3.3. An Unregistered Receiver. An unregistered receiver may have access to private data about the user's family, such as image and video data, which will have a bad impact on the privacy of the user. Besides, once the important timeliness information is received by the unregistered receiver, it is likely to affect the implementation of the IoT emergence measures.

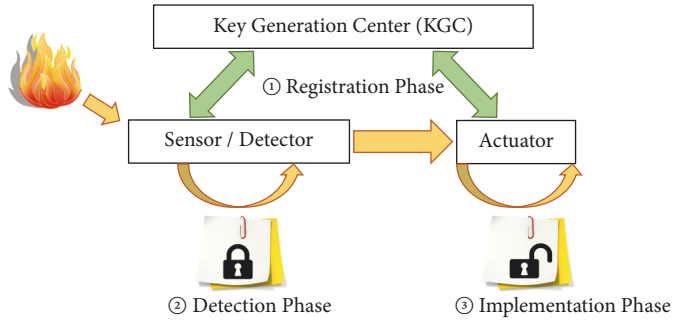

Figure 2: Overview of the proposed scheme.

4. Our Proposed Scheme

In this section, we elaborate on the novel scheme we have proposed. A simple overview of the proposed scheme is presented. On this basis, we describe this scheme in three phases: registration phase, detection phase, and implementation phase.

4.1. Overview of the Scheme. The overview of the proposed scheme is presented in this subsection. Figure 2 shows the visualization of the new scheme in a concise form. The novel scheme is composed of three phases, which are named registration phase, detection phase, and implementation phase. The registration phase is the initial phase of the scheme. The key generation center (KGC) generates private keys of all sensors/detectors and actuators in the network according to their identity information. Note that some necessary offline calculations are completed at this phase to assist in subsequent phases. We will elaborate on the content of these calculations in the next subsection. The detection phase is actually a sign and encryption phase. The subject of the execution is named the sender in our model. The sender represents sensors such as temperature monitor and detectors such as smoke detector and monitoring camera. These devices are responsible for collecting, editing, and encrypting the transmission of detected fire information. This phase requires the security of the collected data that is related to privacy of the family and the message to be sent out in a very short time. The third phase is named implementation phase. This phase is carried out by actuators such as fire extinguishing devices, smart windows, and gas valves. This phase requires that the encrypted data is cracked and the identity authentication of the sender is completed in the very short time, and the corresponding extinguishing operation should be executed accordingly. Through the above three phases, the scheme we provide can accomplish the fast encrypted transmission of emergence information under the IoT environment and accomplish the prevention and response to emergencies.

4.2. Details of the Scheme. The details of the proposed scheme are shown in this subsection.

4.2.1. Registration Phase. The registration phase mainly refers to the process of each node in the network obtaining the necessary information from the KGC. KGC first chooses a secret key t for this system and calculates public key of this system $P_{\text{pub}} = tP$. Generate parameter q_m related to node m's identity information by hash function H_1: $q_m = H_1(\text{ID}_m)$. The private key of the node m is obtained by the calculation of the parameter q_m and the private key t, and the private key is written to the node memory: $s = tq_m$.

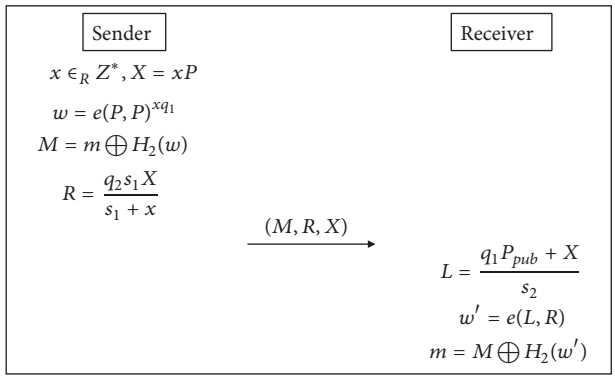

Figure 3: The detection and implementation phase of the scheme.

4.2.2. Detection Phase. The detection phase actually refers to the process of monitoring the abnormal situation by sensors or detectors and compiling these information into files and encrypting the transmission to other nodes. The specific operation process is illustrated in detail in Figure 3.

The sender chooses a random number x, which is a nonzero positive integer, and calculates $X = xP$. Then, the sender computes w:

$$w = e\,(P, P)^{xq_1}\,, \tag{1}$$

where x is the random number and q_1 is the parameter calculated by KGC with the ID value of the sender.

The sender compiles the monitored data into a file named m. XOR operation is performed as follows:

$$M = m \oplus H_2\,(w)\,. \tag{2}$$

The detection result M, which is the encrypted data, is obtained according the above calculation.

Finally, a certification parameter R is calculated:

$$R = \frac{q_2 s_1 X}{s_1 + x}, \tag{3}$$

where q_2 is the parameter computed by KGC according to the identity information of the receiver and s_1 represents the secret key of the sender which is generated by KGC.

Finally, the sender transmits the encrypted detection result M, the certification parameter R, and the parameter X to the receiver.

4.2.3. Implementation Phase. This phase refers to the process of the receiver accepting information and performing related emergence operations. The receiver needs to first authenticate the identity of the node sending the information.

The receiver first computes a assistance parameter L:

$$L = \frac{q_1 P_{\text{pub}} + X}{s_2}, \tag{4}$$

where q_1 is the parameter generated by KGC about the identity information if the sender, P_{pub} is the public key of system, X is the parameter sent by the sender, and s_2 is its own private key.

The parameter w' is restored with the calculation $w' = e(L, R)$. The message about the emergency is computed by $m = M \oplus H_2(w')$.

Finally, when obtaining the correct information, the receiver will implement related operations according to the real-time information.

5. Security Analysis

In this section, the correctness of our scheme is firstly shown. Then, the security analysis is presented in aspects of security against a forged sender, MITM attack, and an unregistered receiver.

5.1. Correctness. The correctness of a scheme is that the calculation process of the design can eventually achieve the desired goal and complete the expected security expectation. For the scheme we have designed, correctness refers to the fact that the sender and the receiver can encrypt and decrypt the information through the methods we design, respectively.

We denote the new w computed by the receiver as w'. w' can be calculated as follows:

$$\begin{aligned} w' &= e(L, R) = e\left(\frac{q_1 P_{\text{pub}} + X}{s_2}, \frac{q_2 s_1 X}{s_1 + x}\right) \\ &= e\left(\frac{q_1 tP + xP}{tq_2}, \frac{tq_1 q_2 xP}{tq_1 + x}\right) \\ &= e\left(\frac{q_1 t + x}{tq_2} P, \frac{tq_1 q_2 x}{tq_1 + x} P\right) = e(P, q_1 xP) \\ &= e(P, P)^{xq_1} = w. \end{aligned} \tag{5}$$

Based on the above deduction, it is not difficult to draw the conclusion that the designed scheme is correct.

5.2. Security against a Forged Sender. An adversary may compromise a sensor node or a detector node to send some fake alarm message. Identity information of the sender might be stolen. Such sender is called a forged sender.

In our scheme, the adversary can fake one ϵ_1 to replace s_1, but he knows nothing about t. So the adversary cannot match his fake ϵ_1 with $s_1 = tH_1(\text{ID})$. Therefore, a forged sender cannot send a R that can be verified.

5.3. Security against MITM Attack. If an attacker wants to capture or tamper with the content of the message by intercepting information, he is called a man-in-the-middle.

The attacker can intercept the message (M, R, X) of our scheme. If he wants to capture the specific message, he needs to decrypt the message M. However, he has no chance to know about the parameter x, which is a random number generated by the sender during every transmission. It cannot be excluded that he can break the message through the receiver. But in fact, an attacker cannot know any recipient's private key s_2.

In addition, if the attacker wants to tamper with the message, he needs to generate a fake number δ to replace the random number x and regenerate R. Actually, he know nothing about s_1, so he cannot generate an effective R. If he even forges s_1, he will fall into the same embarrassment as the adversary in the previous subsection.

Besides, the attacker can constantly collect the encrypted message ciphertext and the original text sent before the sender. However, since x is a random number which changes in every round, he cannot infer the encrypted information from the previous plaintext and ciphertext.

5.4. Security against an Unregistered Receiver. An unregistered receiver is an unlawful node, but it can receive encrypted information. If the receiver is true and not registered, the sender will not be able to compute encrypted information that matches q_2. Therefore, it does not have the corresponding s_2 to decrypt the message.

6. Performance Analysis

This section is going to discuss the performance of the proposed protocol. The computational cost of different entities in the proposed scheme is shown in Table 1. We take into consideration the computational costs of the sender and the receiver. We consider the cost of collision-resistant hash function, bilinear pairing, scalar multiplication, exclusive-OR, and group exponent. In Table 1, M represents scalar multiplication, P denotes bilinear pairing, E refers to group exponent, H represents collision-resistant hash function operation, and XOR denotes exclusive-OR. By computation, the result comes out that a sender costs 2 scalar multiplications, 1 bilinear pairing, 1 group exponent, 1 collision-resistant hash function operations, and 1 exclusive-OR for sending the message to one receiver. In addition, a receiver costs 1 scalar multiplications, 1 bilinear pairing, 1 collision-resistant hash function operations, and 1 exclusive-OR to rebuild the message.

Table 1: Computational cost comparison.

Phases	Sender (Sensor/Detector)	Receiver (Actuator)
Detection Phase	2M + 1P + 1E + 1H + 1XOR	/
Implementation Phase	/	1M + 1P + 1H + 1XOR

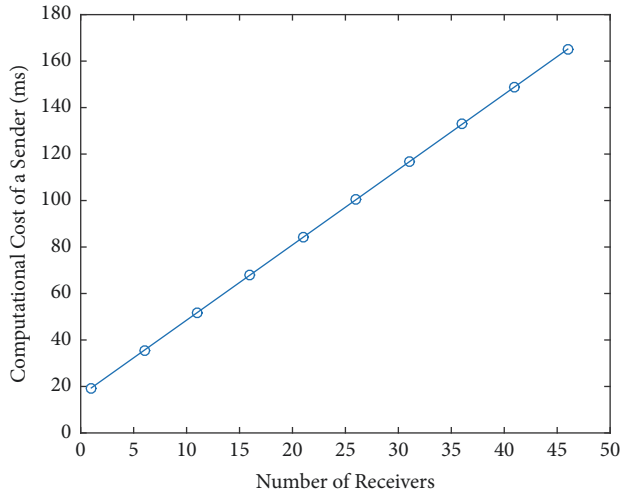

Figure 4: The time cost of a sender when the number of receiver grows.

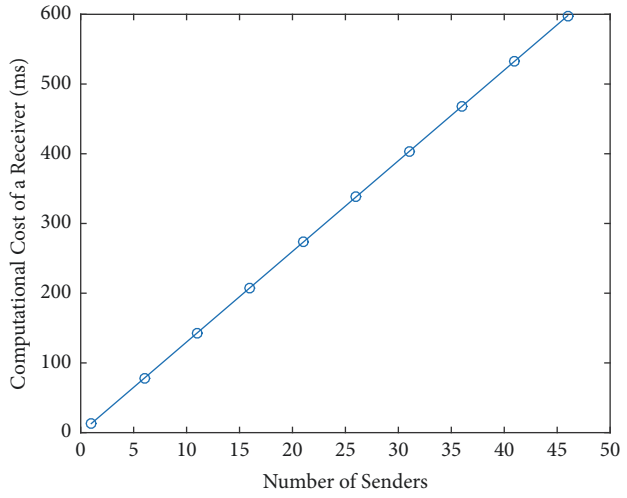

Figure 5: The time cost of a receiver when the number of sender grows.

The efficiency of the proposed scheme is simulated on GNU Multiple Precision Arithmetic (GMP) library and Pairing-Based Cryptography (PBC) library (https://crypto.stanford.edu/pbc/). We utilize C language on a Linux system with Ubuntu 16.04 TLS, a 2.60 GHz Intel(R) Xeon(R) CPU E5-2650 v2, and 8 GB of RAM. The results are illustrated in Figures 4 and 5. It is not difficult to see that both the sender's and the receiver's computational costs will increase as the number of the other party increases. The increasing trend of the sender's cost due to the increase in the number of the other party is slower. Although our experiments simulate a large number of nodes, the number of nodes in a smart home network is actually very limited. Therefore, we find that the new scheme we propose costs very limited time to transmit emergence data. Combining this scheme with efficient data analysis and instruction dispatching algorithms can achieve response to emergencies in a smart home environment.

7. Conclusion

In this paper, we propose a novel scheme based on instant encrypted transmission for IoT-based smart home system. The three phases of the registration phase, the detection phase, and the implementation phase constitute the main part of the overall scheme. The simulation by PBC shows that our novel scheme enables the transfer of important data in a very short period of time while protecting the privacy of data.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant no. 61672295, no. 61672290, no. U1405254, and no. 61772280, the State Key Laboratory of Information Security under Grant no. 2017-MS-10, the 2015 Project of Six Personnel in Jiangsu Province under Grant no. R2015L06, the CICAEET fund, and the PAPD fund.

References

[1] D. Zhang, L. T. Yang, M. Chen, S. Zhao, M. Guo, and Y. Zhang, "Real-time locating systems using active rfid for internet of things," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1226–1235, 2016.

[2] Z. Zhou, M. Dong, K. Ota, G. Wang, and L. T. Yang, "Energy-efficient resource allocation for d2d communications underlaying cloud-ran-based lte-a networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 428–438, 2016.

[3] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[4] X. Zhang, Y. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over volte via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[5] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in

cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, 2017.

[6] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[7] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 64, no. 2, pp. 425–437, 2015.

[8] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 4, pp. 567–580, 2009.

[9] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.

[10] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New Publicly Verifiable Databases with Efficient Updates," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 546–556, 2015.

[11] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, 2018.

[12] M. Z. Alam Bhuiyan, J. Wu, G. Wang, and J. Cao, "Sensing and decision making in cyber-physical systems: the case of structural event monitoring," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 6, pp. 2103–2114, 2016.

[13] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. T. Yang, "Role-dependent privacy preservation for secure v2 g networks in the smart grid," *IEEE Transactions on Information Forensics & Security*, vol. 9, no. 2, pp. 208–220, 2017.

[14] J. Li, Y. K. Li, X. Chen, P. P. C. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," *Parallel & Distributed Systems IEEE Transactions on*, vol. 26, no. 5, pp. 1206–1216, 2015.

[15] J. Shen, C. Wang, C.-F. Lai, A. Wang, and H.-C. Chao, "Direction Density-Based Secure Routing Protocol for Healthcare Data in Incompletely Predictable Networks," *IEEE Access*, vol. 4, pp. 9163–9173, 2016.

[16] Y. Yu, M. H. Au, G. Ateniese et al., "Identity-Based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 767–778, 2017.

[17] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2402–2415, 2017.

[18] P. Li, J. Li, Z. Huang et al., "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, 2017.

[19] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 65, no. 8, pp. 2363–2373, 2016.

[20] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 65, no. 10, pp. 3184–3195, 2016.

[21] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *ComputersSecurity*, vol. 72, p. 12, 2018.

[22] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive and Mobile Computing*, 2017.

[23] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1931–1940, 2017.

[24] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[25] W.-L. Chin, W. Li, and H.-H. Chen, "Energy Big Data Security Threats in IoT-Based Smart Grid Communications," *IEEE Communications Magazine*, vol. 55, no. 10, pp. 70–75, 2017.

[26] L. Chen, S. Thombre, K. Järvinen et al. et al., "Robustness, security and privacy in location-based services for future iot: a survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[27] N. Saxena, S. Grijalva, and N. S. Chaudhari, "Authentication protocol for an iot-enabled LTE network," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, article no. 25, 2016.

[28] M. N. Aman, K. C. Chua, and B. Sikdar, "A light-weight mutual authentication protocol for iot systems," in *Proceedings of the GLOBECOM IEEE Global Communications Conference*, pp. 1–6, 2017.

[29] N. Li, D. Liu, and S. Nepal, "Lightweight mutual authentication for iot and its applications," *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359–370, 2017.

[30] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, "Public key authentication and key agreement in iot devices with minimal airtime consumption," *IEEE Embedded Systems Letters*, vol. 9, no. 1, pp. 1–4, 2017.

[31] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in iot environment," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1634–1646, 2017.

[32] B. L. Parne, S. Gupta, and N. S. Chaudhari, "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network," *IEEE Access*, vol. 6, pp. 3668–3684, 2018.