One Secure IoT Scheme for Protection of True Nodes

Yongkai Fan[1,2(✉)], Guanqun Zhao[1,2], Xiaodong Lin[1,2], Xiaofeng Sun[1,2], Dandan Zhu[1,2], and Jing Lei[1,2]

[1] Beijing Key Lab of Petroleum Data Mining, China University of Petroleum, Beijing, China
fanyongkai@gmail.com
[2] Department of Computer Science and Technology, China University of Petroleum, Beijing, China

Abstract. As a new generation of information technologies, IoT has been applied into many industrial fields and made great contributions to our everyday life. However, vulnerability of IoT constrains the application of IoT, especially, when the node used in IoT systems is malicious one which may break the system and leakage vital data (for example, nodes used by patient to transfer condition data). To tackle the security concerning, we propose one secure IoT framework used to protect true nodes and ensure the secure operation. Firstly, we introduce two types of IoT classic architectures and summarize the security challenges, then we give an introduction and comparison of several IoT security frameworks. At last, we propose our scheme for protecting the safety of IoT nodes in the perception layer.

Keywords: IoT · Security · Security framework · IoT node

1 Introduction

IoT (internet of things) is a novel notion of modern information technologies with no definition in common use yet. The gist of IoT paradigm is the ubiquity of all sorts of objects around us are able to have an interaction with each other and achieve their common goals collectively [1]. In short, IoT represents a linkage between heterogeneous entities which render services in traditional Internet by means of plunking for communications between objects and people. In the current trend of global communication, IoT has gradually evolved into a global "smart object" network [2]. It has also been mentioned that the term IoT represents a technology for interconnecting smart objects into a global network via the Internet [3]. Another definition is that it semantically refers to "the only addressable network of global interconnected objects based on standard communication protocols" [4]. IoT is also known internationally as a "sensor system", that is, a concept of the expansion of sensor networks into objects, and it is also a new revolution of the Internet [5]. In a manner of speaking, IoT delegates a new exposure of informatics.

M. Qiu (Ed.): SmartCom 2018, LNCS 11344, pp. 143–152, 2018.
https://doi.org/10.1007/978-3-030-05755-8_15

IoT has influenced several aspects and has many application scenarios. Here we select representative application areas as examples to show how the IoT exchanges the human living and manufacturing field.

(1) Smart industry. It can provide a more automatic management for better security and effectiveness in a company. For example, hovering the phones on NFC-tagged posters, users can automatically get information from relevant network services and purchase the needed tickets [6]; in addition, ubiquitous computing and sensor technology can make food supply more efficiency [7]. (2) Smart medical treatment. In modern society, high-calories food and decreasing amount of exercise cause a hidden danger on people's health. With the monitoring of wearable devices, the abnormal physical data will be stored in hospitals, which offers a timely information to doctors for potential patients to provide an early protection for users and reduce pressure of medical institution. (3) Smart home. There are many kinds of sensors used on intelligent devices in house, and collected information by sensors is used by individuals who own the network. For instance, a home monitoring system is created by the expansion of computer networks to help doctors monitor their patients. (4) Smart grid. Smart grid has been capable of supplanting the traditional gridline with a view to better service quality. Through the combination of IoT, smart grid can be seen as an intelligent grid delivering electric energy to users, in return consumers can adjust their choices autonomously [8]. (5) Smart transportation. Through the wireless networks, the smart vehicles are able to contact with each other, apperceive and share different traffic information efficiently. Besides, a driver's travel can be scheduled by the intelligent transportation system for better safety, efficiency and reliability. (6) Smart city. It is likely to be a multivariate comprehensive framework, which is used to manage the public affairs of a city through information and communication technology [9]. And as a comprehensive framework, smart city is an integration of different services and applications in one conurbation. (7) Utilities. Applying IoT technologies in gym, the fitness data can be collected and uploaded in time; application in museums can give an automatic explanation in view of conditions of the stream of people, reducing the pressure of management. Public gardens can set up self-regulation systems for plants and public devices by setting proper sensors at all places, offering a better environment for citizens. The water monitoring system use sensors to ensure the quality of people's drinking water, while the electric monitoring system can alter light intensity over time with the use of photo sensors.

From the examples in earlier sentences, we can come to a decision that IoT flourishes our life to a large extent. However, with the popularity of smart devices handling sensitive data, the security considerations related to IoT should not be ignored for the safety and secure utilization of IoT [10]. The remainder of this paper is organized as follows: We first introduce two classic IoT architectures in Sect. 2. In Sect. 3, the security goals and challenges in IoT will be presented in detail. Then we introduce several IoT security frameworks and give a comparison in Sect. 4. Finally, we propose our secure scheme for nodes used in perception layer in Sect. 5.

2 IoT Architecture

According to the recent researches [4, 6, 7, 11, 12], there are two main kinds of architectures of IoT architectures as shown in Fig. 1. The obvious distinction between them is the repartition of layers, as shown in the Fig. 1(a) and (b).

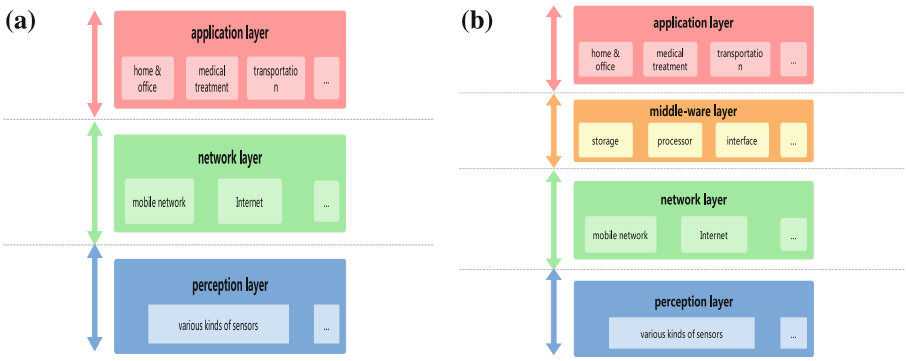

Fig. 1. (a) The three-layer-architecture of IoT. (b) The four-layer-architecture of IoT.

From the Fig. 1(a) [11], we can see that there are three layers in the general architecture of IoT: (1) Perception Layer is also called the sensor layer, which is the bottom of the general architecture. It contains many kinds of sensors, for example, photoelectric sensors, acoustic sensors, infrared sensors or any other kinds of sensor networks. The main propose of perception layer is to identify objects and acquire their status information, store these data and deal with them later. (2) Network Layer is seated in the middle of the general architecture. It is responsible for transmitting, transferring the data collected by sensors in perception layer to different kinds of information processing systems, which through the communication networks. (3) Application layer is the top layer, responsible for realizing different kinds of practical applications belonging to IoT in the light of the users' needs. No matter what kinds of derivative architectures will be constructed in the future, it is necessary to use the three-layer-scheme as a benchmark for improving and achieving.

To build a versatile and flexible IoT multi-level architecture for more functions, a four-layer-architecture which is called as SoA-based architecture is proposed [12]. As shown in Fig. 1(b), middle-ware layer is introduced to connect diverse services or functional units through protocols and interfaces, including information processing systems, which take actions according to the data-processing results. Additionally, it can link the database in which the data storage with the system. What's more, the middle-ware layer is service-oriented that can ensure the same service type among the connected equipment.

3 IoT Security

Although the IoT has brought convenience to human beings, there are also potential security threats and possible attacks. If we want to apply applications or service in IoT safely and effectively, the first thing is to figure out what should we take into consider for the IoT security.

3.1 The Secure Goals of IoT

(1) **Confidentiality.** This characteristic is designed to ensure that only the authorized consumer can access the information. The confidentiality is a crucial security property in IoT because a lot of measurement devices are connected with each other. So, making sure the collected data won't be disturbed or be stolen by other devices for the sake of this aim.
(2) **Integrity.** During the period of data communication, it is important to prevent the sensitive data from being leaked by variety kinds of interference. In IoT, while the applications receive tampered data, wrong operation status can be measured and the system may make a wrong feedback.
(3) **Availability.** Availability is a property which can make sure that the authorized consumer can access the needed data whenever and wherever. Because of the real-time requirements of IoT, the useful information is needed to be transferred timely, unless some services cannot run correctly. Thus, availability is a vital security feature for IoT [6].

3.2 The Security Challenges in IoT

In the consideration of security goals, mail security challenges faced in IoT has to be thought over. We summarize the challenge may be faced and has a simple description of it in Table 1:

Table 1. The main security challenges in IoT.

Challenge	Description
Detection	Either malicious behaviors or malicious nodes will cause a damage in IoT. So, in such a sophisticated circumstance, we need a detection mechanism consisting of two modules. One is intrusion detection while the other is malicious node detection. The proposal of the former detection is finding out abnormal behaviors in all the processing flow and give a feedback for appropriate countermeasures. The latter one aims at chasing down malicious nodes and executing an isolation or clearance
Transmission protection	Because of the inherent limited nature, information leakage is more easily to happen in IoT with tons of data transmitted. An attacker may intercept data in transit and tampering with it, which has an impact on the data integrity and confidentiality. Consequently, people need to take effective methods to avoid attacks during data transmission

(*continued*)

Table 1. (*continued*)

Challenge	Description
Access control	Access control is a kind of authentication for IoT nodes and users, which makes it possible that only the users with effective identity can access specific systems, carry out sensitive operations or gain needed data. When non-permission users call on a visit, the system will reject the request and send a feedback to managers. Some representative mechanisms have been put forward in recent years such as [13–15]. Besides, multifarious access control systems are proposed in view of different principles [16–18]
Recognition	Services and applications in IoT take advantage of received data and meet users' demands. As a consequence, the application layer may cause a battery of security issues without accurate recognition mechanisms, defending untrusted services for trusted users. In most cases, consumers do not have the abilities to distinguish the quality of an application, as anyone is seemed to provide a secured service with delicate camouflage
Data privacy	With the usage of wearable devices and home appliances, more and more private data are stored in intelligent devices or even in cloud. Once there is a physical attack or software flaw, the private information stored can be destroyed or leaked. Therefore, efficacious light-weight security policies need to be put forward for IoT devices with resource and performance constraints

4 Comparison of Several Security Frameworks for IoT

There are some researchers propose appropriate solutions for resisting security threats mentioned in Sect. 3. We select four popular and typical security frameworks or techniques for different fields of IoT to show the security consideration of them. First, we'll give a brief description of each framework and then compare frameworks to show the differences and features of them.

A. Brief Introductions to the Four Frameworks.

(1) Access control system [20]. In this control system, sensors are open to users with mobile devices, and these mobile devices have less ability to track down who is using the resources or data. Here researchers propose an architecture, which is directed against this issue. The proposed framework [20] consists of four parts as Fig. 2(a): the cloud, the mobile clients, the IoT nodes, and the gateway. *The Cloud* plays a role of server, which receives the request from the mobile clients. It can provide variety kinds of services to clients and transmit web requests to IoT nodes. *The Mobile Clients* execute the following function. Once launching to applications, they'll register with the sensors; besides, clients can collect sensor data and initiate authorization requests regularly; what' more, the mobile clients receive the web response and then present it to users. Different *IoT Nodes* have different functions. They can only connect with the gateways, because the nodes only trust the gateway server. *The Gateway* can send usable sensor lists as well as connection requests. If there is any request passed to the sensor, the cloud can know which gateway to choose. Then the specific gateway will

send the information to IoT nodes. (2) Smart cyber infrastructure [19]. Figure 2(b) shows one security framework for IoT, which is used to carry out security developments of intelligent infrastructures [19]. There are four layers in this framework: IoT End Node layer, Network layer, Service layer and Application layer. *End Node Layer* consists of many IoT devices, and the information collected from the real world can be passed to the next layer through this layer. The most significant components in this layer are sensors and actuators. *Network Layer* is designed to conduct data between the end nodes and the fog or cloud. In this layer there is a secure gateway, which is responsible for controlling access to defend against cyber-attacks that might appear. Then the secure data which passed through the gateway can be sent for further processing through networks. *Service Layer* acts as an interface between the next two layers. Because of the lack of memory and computing capacity of IoT devices, all the needed energy and resources are provided as cloud or fog services. *Application Layer* can provide services to devices and users through applications. The most important aspect of the layer is data sharing, so it's of vital importance to avoid information leaks and maintain data privacy. (3) SecIoT [20]. The SecIoT framework (shown in Fig. 2 (c)) is responsible for improving the security in IoT through three modules: authentication, access control and risk indicator. *Authentication* is in the center of the architecture. It connected with data providers and data consumers, so the authentication is divided into user authentication and device authentication. Because the IoT exists in the network ecosystem, providing support for security protocols is crucial, as the security of IoT depends on the realizing degree in some extent. *Access Control* is responsible for identifying whether the users have abilities to access specific data, while the role-based solution is a prevalent mechanism for protecting safety. Different roles are assigned to different users, and thus users with variety kinds of roles can carry out dissimilar jobs. *Risk indicator* can help customers to apperceive security risks better. The security indicator is generated according to asset identification, threat identification and risk evaluation. The asset identification can make sure the asset which should be protected, the threat identification is able to identify the probable threat, and the risk evaluation can evaluate the results and influence caused by threat. (4) Cloud ecosystem [21]. Cloud Ecosystem has three layers called gathering layer, transmitting layer and applying layer shown in Fig. 2(d) [21]. *Gathering Layer* is the bottom of this architecture consisting of sensors and base stations. The sensor nodes have secure localization capability, and can sample, process, communicate complicated data, and send it to the Base station, which acts as a secure gateway. *Transmitting Layer* consists of transceivers and towers, and both of them are responsible for transmitting data between base station and cloud and prevent eavesdropping as well. *Applying Layer*'s main part is the cloud. It can make sure that only the authorized users have the ability to access and avoid privilege escalation.

B. Comparison

After reviewing four typical security frameworks of IoT, we compare them in different evaluation directions in Table 2. Giving a description and comparison of different security frameworks can help people to take appropriate security measures with the necessary technology in different IoT fields.

There are other schemes proposed [16–18] in IoT, they mainly focus on the application layer and network layer, which are responsible for consumer identity and

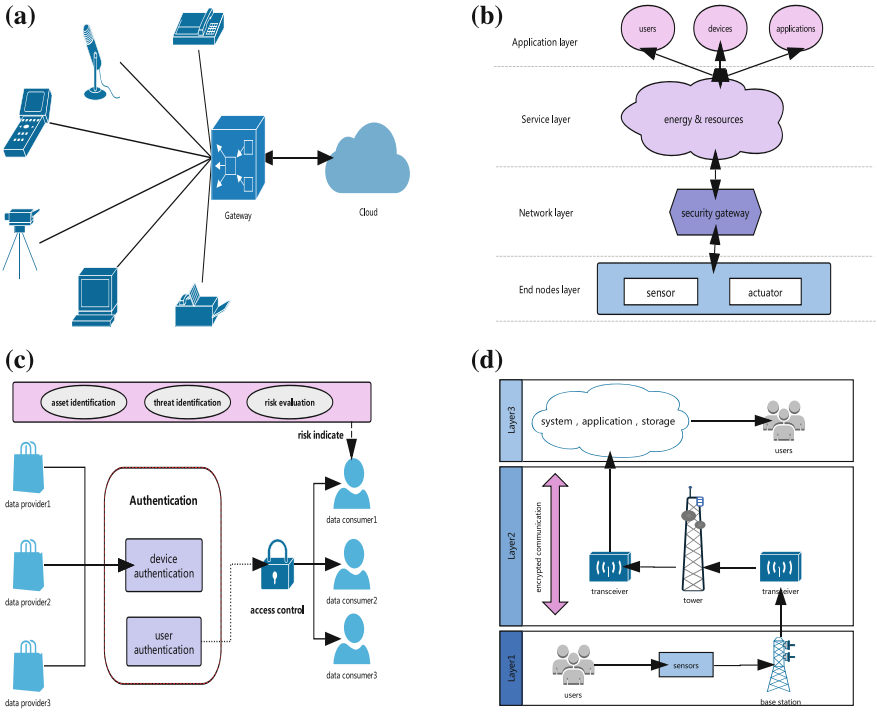

Fig. 2. (a) Access control system. (b) Smart cyber infrastructure. (c) SecIoT. (d) Cloud ecosystem.

data interchange. As a common knowledge, reliable data source is much more important for consideration the security goals we mentioned before, however, there is a short board on the conception layer's security universally. So for the sake of protecting the security of the source data, we put forward a novel scheme.

5 Our Proposal

As we all know, there are many kinds of sensors used in IoT, no matter above mentioned schemes or other frameworks, sensors are used for collecting data from the real world, and then data is transferred and stored for further use. In order to protect the security of the data gathered by sensors, we propose a scheme to give an identification of normal nodes and malicious modes based on several security solutions. The purpose of the scheme is to protect data reliability and security from the beginning of the whole communication process.

The proposed scheme is used in the perception layer between IoT nodes and the key node. There are five main parts in our scheme which is shown as Fig. 3.

(1) **Dacty_Module.** The first step is to extract the unique device information of the IoT node, and then generate a dactylogram of each device. After this process, every

Table 2. Comparison of several security frameworks for IoT.

Framework	IoT component	Security control	Security protocol and technology	Application
A: Access control system	Cloud, gateways, sensors	Null	Web socket, CoAP protocol	Access control of users
B: Smart cyber infrastructure	Cloud, gateways, sensors, actuators	Light-weight encryption, sensor authentication, intrusion detection, anti-jamming strategy, identity authentication, abnormal behavior analysis	Communication protocol for mobile communication network, wireless sensor network communication protocol	Ensure the security of intelligent infrastructure such as the smart home and smart buildings
C: SecIoT	Cloud, sensors	Device and user authentication, role-based access control, risk indication	PKI, out-of-band communication technology, single sign-on mechanism, multi-channel security protocol	Ensure the security of communication between IoT devices
D: Cloud ecosystem	cloud, sensors, base station, storage, communication towers	Access control, identity authentication	Wireless communication protocol, SSDLC, data analysis	Ensure the security of sensors based on the cloud

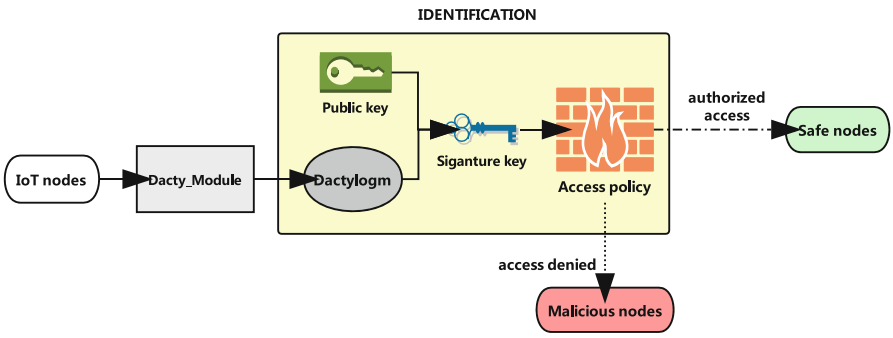

Fig. 3. The proposed scheme in perception layer.

equipment in IoT has a unique identity that will be used as an attribute of the device.

(2) **PKGen_Module.** It will generate a public key for further use. In this step, the system or the trusted third party will produce a public key with some parameters. The public key is used for generating a signature key in the next step.

(3) **SKGen_Module.** The main goal of this module is generating signature key. Here we use the public key along with the dactylogram produced in the first step to carry out the process. As a result, the dactylogram will be a part of the signature key as an attribute.

(4) **Sig_Module.** Here, the system will sign collected data with the public key and the signature key. Here we need to define an access policy, in which there are security nodes' dactylograms included. Of course, the malicious nodes' dactylograms are not in the policy. After that, we use the signature key with the unique dactylograms to sign the collected data.

(5) **Verify_Module.** In the last step of our scheme, the module will carry out a verification on the basis of previous steps. Using the public key, signature key and defined access policy to verify the device's identify. The principle is if the attribute in signature is a part of the policy, the device is safe. Otherwise, the device is considered as a malicious node and access denied.

We are still on our way to do some extensive experiments; the proposed scheme seems useful and effective according to our initial experimental results. Moreover, security analysis is under its way and there are lots of work need to be done in order to make sure our proposed scheme can meet the security requirement.

6 Conclusion

IoT has the advantages of high efficiency, low cost, and high scalability. With the development of IoT, security issues have become more serious. Because people put great emphasis on services provided by the IoT environment, safety issues have not led to adequacy attention. This article introduces IoT security-related knowledge and introduces four different security frameworks in IoT. In addition, we give a brief comparison of them, and then introduces our new scheme simply. Our future work will focus on the theoretical analysis and extensive experiments to prove our scheme can be a useful and improvement of security goals in IoT.

References

1. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
2. Giusto, D., Iera, A., Morabito, G., Atzori, L.: The Internet of Things. Springer, New York (2010). https://doi.org/10.1007/978-1-4419-1674-7. ISBN 978-1-4419-1673-0
3. The Internet of Things, ITU Internet Reports (2005). http://www.itu.int/internetofthings/

4. INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nano systems. In: Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, 27 May 2008
5. Vermesan, O., et al.: Internet of things strategic research and innovation agenda. River Publishers Series in Communications, p. 7 (2013)
6. Maheswari, S.U., et al.: A novel robust routing protocol RAEED to avoid DoS attacks in WSN. In: 2016 International Conference on Information Communication and Embedded Systems (ICICES). IEEE (2016)
7. Ilic, A., Staake, T., Fleisch, E.: Using sensor information to reduce the carbon footprint of perishable goods. IEEE Pervasive Comput. **8**(1), 22–29 (2009)
8. Siano, P.: Demand response and smart grids—A survey. Renew. Sustain. Energy Rev. **30**, 461–478 (2014)
9. Hao, L., et al.: The application and implementation research of smart city in China. In: 2012 International Conference on System Science and Engineering (ICSSE). IEEE (2012)
10. Fan, Y., Liu, S., Tan, G., et al.: Fine-grained access control based on trusted execution environment. Futur. Gener. Comput. Syst. (2018)
11. Mahmoud, R., et al.: Internet of things (IoT) security: current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE (2015)
12. Xu, L.D., He, W., Li, S.: Internet of things in industries: a survey. IEEE Trans. Ind. Inform. **10**(4), 2233–2243 (2014)
13. Anggorojati, B., et al.: Capability-based access control delegation model on the federated IoT network. In: 2012 15th International Symposium on Wireless Personal Multimedia Communications (WPMC). IEEE (2012)
14. Chen, H.C.: Collaboration IoT-based RBAC with trust evaluation algorithm model for massive IoT integrated application. Mobile Netw. Appl., 1–14 (2018)
15. Sanchez, P.M., Lopez, R.M., Skarmeta, A.F.G.: PANATIKI: a network access control implementation based on PANA for IoT devices. Sensors **13**(11), 14888–14917 (2013)
16. Pereira, P.P., Eliasson, J., Delsing, J.: An authentication and access control framework for CoAP-based internet of things. In: IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society, pp. 5293–5299. IEEE (2014)
17. Bernabe, J.B., Ramos, J.L.H., Gomez, A.F.S.: TACIoT: multidimensional trust-aware access control system for the internet of things. Soft. Comput. **20**(5), 1763–1779 (2016)
18. Guoping, Z., Wentao, G.: The research of access control based on UCON in the internet of things. J. Softw. **6**(4), 724–731 (2011)
19. Monir, S.: A Lightweight Attribute-Based Access Control System for IoT (2016)
20. Huang, X., Craig, P., Lin, H., et al.: SecIoT: a security framework for the internet of things. Secur. Commun. Netw. **9**(16), 3083–3094 (2016)
21. Rahman, A.F.A., Daud, M., Mohamad, M.Z.: Securing sensor to cloud ecosystem using internet of things (IoT) security framework. In: Proceedings of the International Conference on Internet of things and Cloud Computing, p. 79. ACM (2016)