Application of identity-based cryptography in IoT services

Jiang Yali[1,a], Kong Fanyu[1,b], Bai Shundong[2,c]

[1]Network & Info Security Institute, Shandong University, Jinan, China

[2]Shenzhen Aolian Info Security Co., Ltd., Beijing, China

[a]jiang.yl@sdu.edu.cn, [b]fanyukong@sdu.edu.cn, [c]baisd@myib.cn

Keywords: IoT, Identity Based Cryptography (IBC), security

Abstract: The IoT brings us more convenience and higher efficiency, at the same time it brings people more danger. How to keep IoT secure is the most important task. Identity Based Cryptography (IBC) has special advantages and simple key management. IBC is more suitable than the other cryptography technology to provide security services for IoT.

1. Introduction

With the development of intelligent devices, millions of things connect with each other over internet in our daily life. The Internet of Things (IoT) becomes the reality from a concept. The IOT brings us convenience and high efficiency. At the same time much private information and secret are divulged because of IOT. It is reported that many cameras installed in families were hacked by CCTV in 2017. Their privacy of daily life were snooped and broadcast through network. Recently massive assaults launched by hackers from devices of IoT arise again and again. Several DDoS attacks were reported in American in 2016 [1]. More and more intelligent cars are added into the IoT. More and more danger are hidden in them. When the intelligent systems of the cars are attacked, all the function will be controlled by hackers, start, pause, shutdown etc. included. Intelligent cars turn out to be life-threatening. IoT is also included in national infrastructure and military field even. So how to keep IoT secure is the most important task.

2. Why IoT can be attacked easily?

First, IoT is composed of many kinds of smart devices. Software and hardware of these devices are different from each other. These devices were designed and manufactured without security initially. The storage space and computational power of these intelligent ends are limited. So it is hard to deploy security software and high-complexity cryptography schemes into these equipments. As the sensing layer, intelligent devices are mainly in charge of collecting information. The information is usually important and sensitive to the user or organization. Most data isn't protected when it is stored in devices or transported over the network. So the data can be detected by the hacker.

Secondly, the users of IoT focus on the availability and convenience, not on the security. At the same time, to keep secure can't pay the price of convenient availability. So both the users and manufactures ignored the secure factor.

Thirdly, IoT lacks the uniform administration. The security of protocols for telecom networks in IoT is limited. Some devices set the self-defined network protocol. Most Information transported over the IoT are encrypted simply. The information can be got and altered and deleted by attackers.

It is common that things of IoT were made by different vendors. There wasn't uniform standard to authenticate the ends of IoT. Traditional authentication and authorization is performed on the users, not on the devices. Most intelligent ends use vulnerable password or default accounts and according password. So much as some devices needn't any identification. So the hacker can access these devices easily.

Copyright © (2019) Francis Academic Press, UK DOI: 10.25236/isaicn.2019.075

3. How cryptography can be used to keep IoT secure?

There are many security threats in IoT such as software security, hardware security, telecom protocol security, data security, privacy divulge and so on. So many new measures and security products should be made to keep IoT secure.

In this paper, we only discuss how cryptography can be used to keep IoT secure.

Cryptography is widely used in information security to provide services like data confidentiality, data integrity, authentication and non-reputation etc. These services have been exploited in traditional internet especially in e-commerce. Data confidentiality, integrity, authentication, and access control are the essential services required for securing IoT.

Cryptography schemes are divided into symmetric-key and public-key cryptography according to the keys used in them. Both symmetric-key and public-key cryptography have been studied to be used in IoT[2][3].

The symmetric-key cryptography is relatively simple, but it does not suitable for the IoT. As The symmetric-key cryptography can only provide data confidentiality service. And the symmetric-key mechanisms need pre-sharing a pair of secret key among devices before communication. It is hardly possible to communicate with the parties in other IoT system without the corresponding secret key.

Public key cryptography can accomplish all the security services mentioned above. Public key system use a pair of key which includes public key and private key to resolve the key sharing problem in symmetric-key cryptography. The Certificate-based Public Key Infrastructure (PKI) is the common form used in the traditional internet. Public key is issued as a certificate with the information of the subject publicly. Private key is kept by the subject. A PKI system involves heavyweight key management operations, such as certificate issuing, distributing, querying, updating, verification, and revocation etc. Although PKI is relatively mature and stable, such system can't fit the need of IoT . With the increment of the devices, massive certificates for them will be issued and managed. PKI systems will consume too much resource to maintain normal performance. Limited storage space of the device is not enough for certificate and computation. The narrow communication band of the NB-IoT networks also causes problems when certificates exchanging in security protocols.

To solve the problem of the public key management in PKI systems, Shamir proposed another type public key cryptography defined as the identity-based cryptography (IBC) in 1984 [4]. An IBC system is lightweight and more suitable for IoT than a PKI system.

4. What is the IBC?.

Identity-based cryptography chooses an entity's identity as a public key instead of generating a random pair of public/private keys and issuing the public key in a certificate. Any identity string which can uniquely identify the user or the device can be directly used as a public key, such as e-mail address, identity number, telephone number, domain name, device ID, IP address and so on. A private key generator (PKG) as a trusted party is responsible for generating the private key corresponding to the identity. The private key is issued to the entity when he first joins the network. All private keys needn't be stored and managed in the PKG. So an IBC system is lightweight. In an IoT, everything has a unique identifier. IBC can be exploited directly by using identifiers as public keys in an IoT . When a new device is first added into an IoT system, the trusted center PKG will generate the private key according to the device identifier and issue the key into the device. The Ends of an IoT system can communicate with each other without pre-exchanging public keys. Problems of device storage and narrow band of security protocols are solved by using the IBC without degrading performance of an IoT. IBC scales well to both the high number of endpoints and the diversity of the devices because of the simple key management.

TABLE I. Comparation between PKI AND ibc

Factors	PKI	IBC
Security	High-level	High-level
Encryption	Hard, Certificate should be prepared.	easy, Multiple type encryption is supported
Decryption	Easy at the client end Hard at the server end	easy, It Needn't pre-register.
CrossDomain communication	Hard, The cross-domain certificate chain is needed.	Easy, Publishing the public parameter is needed.
Components corporation	Complicated and hard	Easy
Extensibility	Hard	Easy
Application Scene	Third party authentication	Mass entities. End to end communication IoT, Cloud computation.

5. How does an IBC system work?

Like the other type of public key cryptographic system, an IBC system provides a set of schemes including Identity Based Encryption (IBE), Identity Based Signature (IBS), Identity-Based Authenticated Key Agreement (IBAKA) to provide confidentiality, authentication, secure channel, etc.

To setup an identity based cryptology system, a PKG should be set and initialized first. This initialization procedure is defined as IBCInit. Given a security parameter, a set of system parameters (sysparam) are determined and a pair of master keys defined as master public key (mpubk) and master private key (mprivk) are generated in IBCInit function. The system parameters set and the master public key are composed together and published as the public parameters (pubparam) of the IBC system. The master private key (mprivk) is kept secretly by PKG.

When a new entity is added into the IBC, a key generation function defined as IBCExtr will be invoked by PKG. This function generates a private key (privk) from the identifier of the entity with the public parameters (pubparam) and the master private key (mprivk). The PKG can issue the private key (privk) to the entity online or offline depending on the system requirement. When the above keys are prepared, ends of the system can communicate securely with each other.

If the communication needs authentication, IBS scheme is used. Each end signs the message m with its own private key (privk) by invoking the signature function (IBCSign) and then sends the signature (m, s) to the opposite entity. When receiving the signature (m, s), the receiver invokes the verification function (IBCVerify) to verify the identity of the opposite with the pubparam.

When the communication should be confidential, **IBE** scheme is used. The message m transported between two parties will be encrypted into the cipher c by the encryption function (**IBCEnc**) with the opposite identity and the pubparam. When the cipher is received, each party gets the plaintext m by invoking the decryption function (**IBCDec**) with its own private key (privkey).

All the functions in an IBC system is listed below:

IBCInit: Given the security parameter of the system, to create the public parameter and master private key.

Input: security parameter

Output: pubparam, mprivk

IBCExtract: To generate private key for the according entity.

Input: pubparam, mprivk, ID

Output: privk

IBCSign: Using the party's private key to sign the message m to be authenticated.

Input: pubparam, ID, privk, m

Output: s

IBCVerify: To verify the signature of the opposite party using his ID

Input: pubparam, ID, m, s

Output: valid or invalid

IBCEnc: To encrypt the message using the opposite entity's ID before sending message.
Input: pubparam, ID, m
Output: c
IBCDec: Using its own private key generated by PKG to decrypt the cipher received.
Input: pubparam, ID, privk, c
Output: m or error

There are a few international and national standard algorithms for identity-based cryptography, such as BB1-KEM and BF-IBE[5], SM9-IBE and SM9-AKA [6], SM9-IBS, Cha-Cheon-IBS and Hess-IBS[7] and so on. All these algorithms are based on the discrete logarithm assumption over an elliptic curve.

The integral process of IBC services is described in the Figure 1.

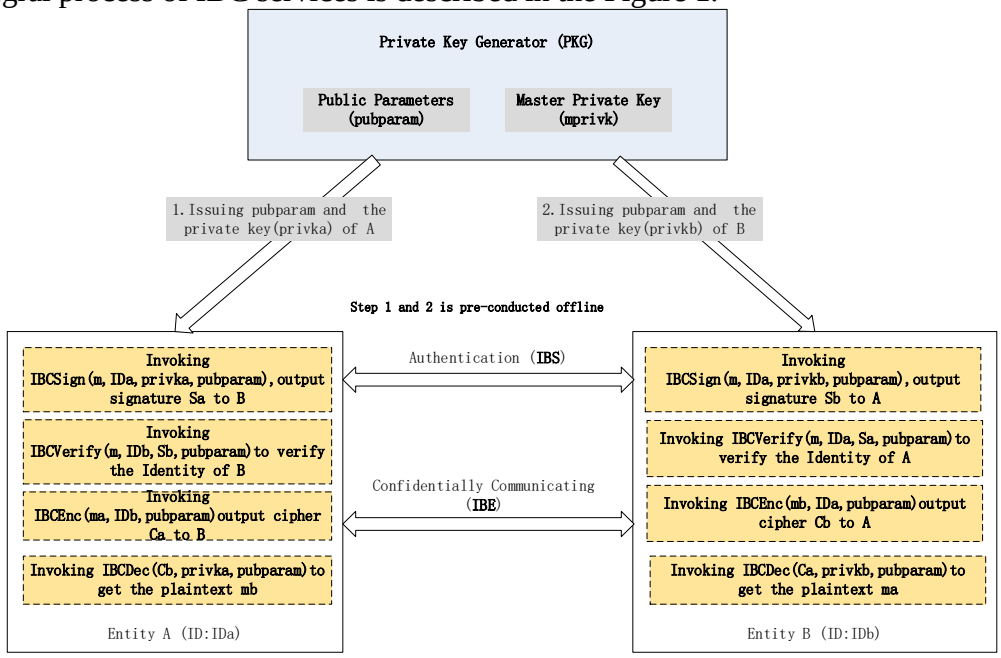

Fig.1 Processes of the IBC services

6. How IBC can be used in the IoT?

A typical IoT system is constructed by three layers: entity/device layer, channel layer, cloud service layer. The entity layer is composed by all the things of the IoT such as household appliances, cameras, cars and mobile phones etc. All the information collected from the device layer is transported to the cloud service layer through channel layer. The IoT cloud servers provide service such as device management, information service, data analysis and user access etc.

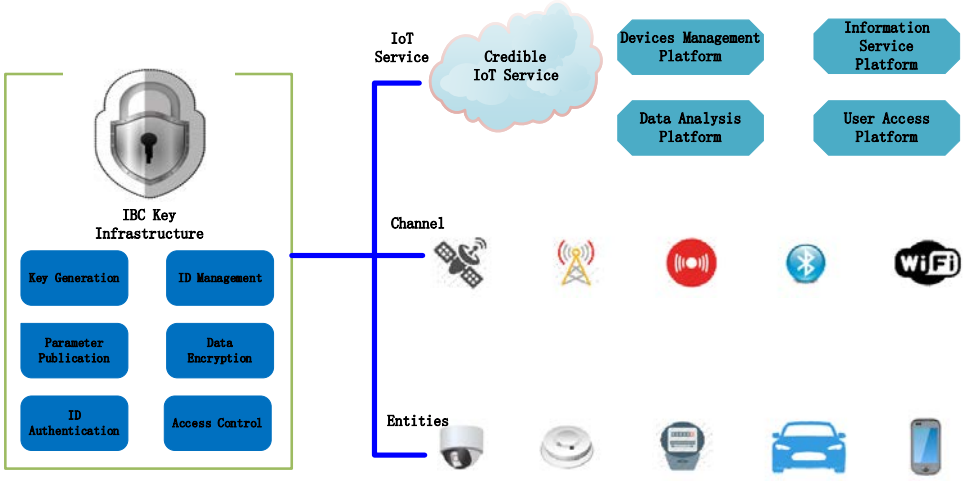

Fig.2 Structure of the IoT system based on IBC key infrastructure.

To support an IoT system secure, a uniform IBC key infrastructure needs to be deployed, cryptographic machine, key administration platform, secure middleware etc. included. The structure of the IoT system based on the IBC key infrastructure is described in the Figure 2.The main functions and SDK of the infrastructure include the following function modules.

- **Private key generation:** It is responsible for deriving the private key from the related entity's ID and issued the private key to the entities. It is mainly corresponding to the IBCExtract procedure mentioned above.
- **Parameter publication:** It issues the public parameter of the IBC key infrastructure to the entities of the system. It also supports the clients to inquire the public parameter when they need. The public parameter is generated in the IBCInit primitive.
- **ID management:** All the ID of the entities allowed to access the IoT system are administrated uniformly by the function module. The IDs are stored, published and updated etc. in the infrastructure.
- **ID authentication:** The module provides the function and SDK to support the ID to be authenticated when the IoT system needs. It mainly includes the IBCSign and IBCVerify procedure of the IBS scheme. The sender invokes the IBCSign with the private key to sign the message it sends. The receiver authenticates the sender by invoking the IBCVerify with the sender's ID as the input parameter. The usage of user ID authentication is the same as the device ID authentication.
- **Access Control:** It remains the map lists of the entity ID and the resources the entity has the right to access. It also administrate the user's access right When an access occurs, an access control begins to run.
- **Data Encryption:** It provides the function and SDK to ensure security of the sensitive or confidential information transported in the IoT system. It mainly includes the IBCEnc and IBCDec primitive SDK. Three layers of the IoT system need to support and use the SDK to keep communication secure.

The IoT system works securely based on the IBC key infrastructure. With the IBC mechanism, all the devices in an IoT system can be authenticated. A security chip can be added into a device to support the IBC computation or the new SDK is added to exploit IBC schemes in the form of software. Before a new device joins in a new IoT system, the private key related to its ID and public parameter of the secure infrastructure will be issued into it. When the device joins in an IoT system, the IoT cloud server authenticates the device by the ID authentication function module. The IBC system supports different type of devices. All the devices belong to a user are administrated by the user with the APP installed in the user's smart phone. The user is authenticated when he login the APP. All the users are administrated in the user access platform deployed in the IoT cloud services with the support of access control function of the key infrastructure.

The channel layer can support secure communication by using the key exchanging protocol and data encryption module.

The cloud servers of an IoT system use the secure foundation provided by the IBC key infrastructure to supply the services credibly.

- **Device management:** When the devices are all authenticated, the management of the devices of the IoT is credible.
- **Information service:** All the information comes from the known and controllable sources because
  of authentication and access control operation, so the information service is credible.
- **Data analysis:** Based on the security of the devices and channels, the data analysis is credible.
- **User access:** With the user ID authentication and access control policy, user in the IoT is credible and is allowed to access the system.

7. The key's operation in the IoT system

In the secure IoT system, the most important part is the key infrastructure. In the key infrastructure, the most important task is the keys' administration. The main operations of the key

include generation, distribution, storage, usage, update and revocation etc.

Whether in the IoT system layer, or in the devices, or in the user client , public parameter, device ID, device private key, user ID, user private key are used and administrated. The key's operation is desribed below.

- **Public Parameter**: It is generated by PKG and issued to the device when the device private key is generated and issued. The parameter is published. It needn't to be stored securely. The public parameter is used when the device computes the public key. When the system updates, the parameter updates. It needn't to be revoked.
- **Device ID:** It is generated and distributed by the IoT system uniformly. It is public and needn't to be stored securely. It is used in the public key computation, identity verfication and data encryption. The device ID needn't update and be revoked.
- **Device Private Key:** It is generated and issued by the PKG offline. It is stored and protected by the user's thumbprint in the device and not in the PKG. It is used to sign the message to confirm the identity，to decrypt the cipher received. It needn't update. When It need to be revoked, the private key file in the device is deleted.
- **User Identifier:** It is owned by the user originally,such as telephone number, e-mail address. When the user registers in the system, the user identifier is sent to the system and administrated by the server. It is stored in the system database securely. It is used to genenrate the public key,encrypt the data, and verify the corresponding identifier. It needn't update and be rovoked.
- **User Private Key:** It is generated and issued by the PKG offline. It is stored and protected by the user's thumbprint in the user's device. It is used to sign the message to confirm the user's identity, to decrypt the cipher received. It needn't update. When It need to be revoked, the related key file is deleted.

8. Conclusion

The nature feature of the IoT, that everything of the IoT has a unique identifier just fits the nature feature of identity based cryptography. Their good combination will bring the world more security and more peace.

References

[1] Internet of Things Smart Device Information Security White Paper. China institute of electronic standardization 26/12/2017

[2] The Perception Layer Information Security Scheme for Internet of Things based on Lightweight Cryptography [J]. Hu Xiangyi, Xu Guanning, Du Liping Network Security. 2013.3

[3] The New lightweight Digital Signature Scheme [J]. Wang Houzhen, Zhang Huanguo. Journal on Communications. 2010.

[4] Adi Shamir, Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53, 1984

[5] X. Boyen and L. Martin. Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems. RFC 5091, December 2007

[6] GM/T 0044.2-2016, Identity-Based Cryptographic Algorithm Using Bilinear Pairings. 2016.

[7] ISO/IEC. Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms. 2016.