Dynamic Cipher for Enhanced Cryptography and Communication for Internet of Things: A Review

SweetyBansal[1], NavneetVerma[2]
Research Scholar, CSE Department, GEC, Panipat[1]
Head of Department, CSE Department, GEC, Panipat[2]

***Abstract*-With the development of Internet of Things (IOT), there are more and more concerns about the security of IOT. In terms of security of Internet, the security framework of Internet cannot provide a completely solution to solve all security problems in IOT [1]. This paper describes the security structure of sensor layer ,network layer and application layer in IOT. This thesis intends to analyze the security features of sensor layer and then presents dynamic variable cipher security certificate, a new method of ID authentication among node and node in sensor layer. This certificate provides a method of "one time one cipher" between communicating parties. It's a lightweight encryption or decryption method, using time stamp technology, timeliness in the two communication partners is guaranteed. In general, dynamic variable cipher security certificate can be well applied to the communication among sensor nodes in IOT.**

Key Words: - Cipher; Authentication; IOT.

I. INTRODUCTION

With the background of Internet, the Internet of Things (IOT) is an emerging technology combining RFID technology, wireless communications technology and EPC standard and so on [2]. In IOT, all things will share the real-time information from all over the world. With the development of IOT, its security problems became more apparent. The Internet is not safe, it could be worse, which will provide wide space and rich chances for cyber attackers in the random distribution sensor network and the whole wireless network. [3]The research and application of IOT is still in its early stages, many of these theories and key technologies should be breakthrough [4]. For security of IOT, Most security mechanism of present network security structure can provide some security mechanisms such as authentication mechanism, encryption mechanism. But it should be redesigned According to its characteristics in IOT. Dynamic variable cipher security certificate presented in this article is a safe variable key authentication protocol based on request-reply mechanism. It has characteristics like "one time one cipher", real-time performance on timestamp, highly efficient data stores the computational burden is low. It can be widely used in the authentication process of Near Field Communications.

Nowadays, around two billion people around the world use the Internet for browsing the Web, sending and receiving emails, accessing multimedia content and services, playing games, using social networking applications and many other tasks. While more and more people will gain access to such a global information and communication infrastructure, another big leap forward is coming, related to the use of the Internet as a global platform for letting machines and smart objects communicate, dialogue, compute and coordinate. This has given rise to new opportunities for the Information and Communication Technologies (ICT) sector, paving the way to new services and applications able to leverage the interconnection of physical and virtual realms. In this paper we will discuss various IoT security issues and Cryptographic Services to solve such issues. The paper is arranged as follows: The second section mainly introduced the security framework of IOT and security problems of sensor layer. The third section mainly expounds the design idea of dynamic variable cipher and the authentication process of dynamic variable cipher security certificate. The fourth section described an application of dynamic variable cipher security certificate, then We analyzed the test results. The fifth section is the summary of this paper.

II. SECURITY OF IOT

2.1 Security framework of IOT

Summarized in nature, IOT can be reflected in the following three aspects. Firstly, any object in the world is connected to Internet; it means that nodes will communicate easily with each other. Secondly, all around sensing, It means that any object in IOT could be identified automatically. The third is intelligent processing, these are characterized by automation, self-feedback, intelligence control etc. The second and the third are kernel contents of IOT. Seeing from the entire security system of the Internet of Things, there can be three layers, including the Sensor Layer Security, the Network Layer Security and the Application Layer Security. The core of IOT security includes safely information sensing, reliable data transfer and safely information control. As you can see from the diagram Figure 1,

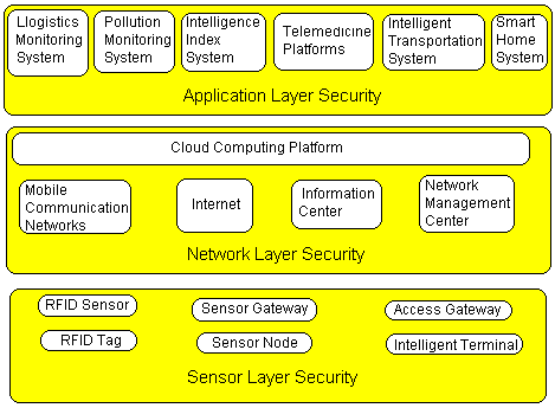

Figure 1 Security framework of IOT

In this layered architecture, the security mechanism of IOT must be designed based on key technologies possibly adopted in each layer and which security threats it faces.[5] The Sensor Layer is at the most frontend of information collection, which plays a fundamental role in the IOT security.

2.2 Security issues in sensor layer

On contrast with traditional network sensor nodes in IOT deployed in an unattended environment, there are some new characteristics in sensor network.

1) Wireless link signal is very weak

Sensor nodes transmit data to each other mainly by wireless network [6], and most of them are work in low power and long time environments. During the wireless communication, it's signal usually affected easily by the disturbing waves [7]. So it is not safe to transfer information by wireless network.

2) Node is exposed

As wireless channel is an open and shared channel, there are hidden terminal and exposed terminal problems in the wireless data communication [8]. For example, when use RFID technology in sensor layer, the object which embedded a RFID chip will be censored not only by its owner but also by others, then the sensor node is the best place for attackers.

3) Network topology is dynamic

Positions of IOT node often change from one place to another place. Compared with traditional TCP/IP network, all network monitoring technologies or cyber defense technologies have to face more complex network data, more strictly real-time demand [9]

4) Limited computing capacity, storage capacity energy

Usually, IOT node is a product of low power consumption, its computing capacity, storage capacity energy are limited [10]. So security technologies of traditional network can not transplant to IOT smoothly

.

2.3 Security technology in sensor layer

1) Encryption mechanism

Cryptosystem is the foundation of information security. In traditional network, there are two uppermost forms of cryptographic applications. Point to point encryption and end to end encryption. As we know from the IOT framework. Generally, the node of sensor layer is low speed CPU such as single chip system [11]. Encrypt and decrypt programs can not use large storage and high power. So Encryption mechanism in IOT should be lightweight.

2) Access control

In IOT, some new connotations are added to access control mechanism. In TCP/IP network, the role who should be authorized to access the system is "person", but in IOT, it is "machine" [12]. So it need to assign and transfer sharing data self-determine between node and node.

3) Authentication mechanism of nodes

Authentication mechanism is used in receiver to ensure the true identity of sender, and ensure whether the data is changed during the transmission. From the point of IOT architecture, It is very necessary that deploy an authentication mechanism in sensor layer.

Authentication can ensure the true node is working, Encryption mechanism can keep the data confidential by encode the data, it can prevent intruder from stealing and tampering crucial information by applying data encryption [13].

III. PRINCIPLES OF DYNAMIC VARIABLE CIPHER SECURITY CERTIFICATE

3.1 The design idea of dynamic variable cipher

Dynamic variable cipher security certificate is a variable key security authentication protocol based on request reply mechanism. As shown in Figure 2, you can see its principles; there is the same key matrix in all communication parties.

	1	2	3	4	5	6	7	8
A	34gg	fve5	54f4	4c57	5658	ad65	58gd	4534
B	4atf	4a4a	45dh	45ac	5e5g	54de	vw5s	5egw
C	hsfs	dv6d	345d	ef2f	45bt	4eds	4de3	4fgw
D	k4fs	s3g4	56gg	da45	vfgw	54gg	4dg4	afa3
E	jf3t	3afv	3fad	3dfv	5xag	45sa	hfy4	ddff
F	Ujk4	4aav	4geg	4fd4	dq53	45sw	gwtx	4a45
G	32gl	4a45	3fad	cts6	sg55	dg5g	36f8	gf34
H	o36g	ddfg	sfey	ef4t	ca45	gf85	gsdh	w3gr

Figure 2 Key matrix

The storage space of the key matrix are 8*8*8=256 Bytes. The communicating parties will randomly generate a coordinate from 1 to 16 bit length. Then according this coordinate, we will get a random password, and it's length can be 4Bytes to 256Bytes,sothere are be 64!=1.26*1089 password in theory. It is realizes truly "one time one cipher". The communicating parties only transfer it's key coordinate and not the key itself .All it's work provides security for the communicating parties through "one time one cipher" which dynamically composed by random coordinate and key matrix .

IV. THE AUTHENTICATION PROCESS OF DYNAMIC

variable cipher security certificate

The authentication process of dynamic variable ciphersecurity certificate is shown in Figure 3. A and B are two nodes of communication. Their clients and servers are relative.

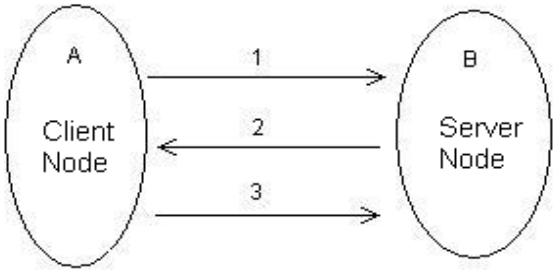

Figure 3 The authentication process of dynamic variablecipher security certificate

The process are as follows:

1. A →B : $Pos\_{x_1,y_1}, E\ (K_{ab1}: ID_a, Cmd, Ta1)$
2. B→A: $Pos\_{x_2,y_2}, E\ (K_{ab2}: ID_b, Cm\_x\_y, Ta1, Tb1)$
3. A →B : E (

Where ID_a ,ID_b means ID number of node A and node B, Cmd means connection request, Pos_x_y means coordinate of key matrix, Ta and Tb means timestamp of node A and node B. E(kab:m) means using password kab to code message m, Text means message constant. As we can see from the description above, client A send an encrypted information of ID_a, a connection request and timestamp Ta1 ,at the same time client A start a timer waiting for some feedback from server B. If no echo reply is received, then A will cancel this session.

When some information arrived server B, it will verify the ID_a from node A. If A is validity, then server B send an encrypted information to A which include ID_b, coordinate of key matrix, timestamp Ta1, timestamp Tb1, at the same time client B start a timer waiting for some feedback from client A. If no echo reply is received, then B will cancel this session.

When some information arrive client A, it will verify the Ta1 from node B. If B is validity, then A gets a communication password Kab according coordinate of key matrix. Next, A generates a new timestamp Ta2,combine with Tb1 and sending message constant. All these data will be sent to server B. Up to this point, we have set up a channel between communicating parties.

The data transferring should use fixed password or one time one cipher.

V. ENCRYPTION MECHANISMS

In the traditional network layer we adopt by-hop encryption mechanism, in this way the information is encrypted in the transmission process, but it needs to keep plaintext in each node through the decryption and encryption operations. Meanwhile in the traditional application layer encryption mechanism is end-to-end encryption, that is, the information only is explicit for the sender and the receiver, and in the transmission process and forwarding nodes it will be always encrypted.

In the IoT network layer and application layer connect so closely, so we should choose between by-hop and end-to-end encryption. If we adopt by-hop encryption, we can only encrypt the links which need be protected, because in the network layer we can apply it to all business, which make different applications safely implemented. In this way, security mechanism is transparent to the business applications, which gives the end users convenience. In the meantime this brings the features of the by-hop full play, such as low latency, high efficiency, low cost, and so on. However, because of the decryption operation in the transmission node, using by-hop encryption each node can get the plaintext message, so by-hop encryption needs high credibility of the transmission nodes.

Using the end-to-end encryption, we can choose different security policy according to the type of business, thus it can provide high level security protection to the high security requirements of the business. However, end-to-end encryption cannot encrypt the destination address, because each node determines how to transmit messages according to the destination address, which causes it cannot hide the source and the destination of the message being transmitted, and bring about malicious attacks.

Through the above analysis, we can draw a conclusion: when the security requirement of some business is not very high, we can adopt by-hop encryption protection; when the business needs high-security, then end-to-end encryption is the first choice. So, according to the different requirements we choose alternative encryption mechanism.

Currently, IoT is developing in its primary phase, and the research of safety mechanism is in the blank in the practice, so we have a long way for the research of this domain.

Cryptographic Algorithms

So far there is a well-known and widely trusted suite of cryptographic algorithms applied to internet security protocols such as table 1.

Table 1. A SUITE OF CRYPTOGRAPHIC ALGORITHMS

Algorithm	Purpose
Advanced encryption Standard (AES)[8]	Confidentiality
Rivestshamiradelman (RSA)/ Elliptic curve cryptography (ECC)[9][10]	Digital signatures key transport
Diffie-hellman (DH)[11]	Key agreement
SHA-1/SHA-256[12]	Integrality

Usually the symmetric encryption algorithm is used to encrypt data for confidentiality such as the advanced encryption standard (AES) block cipher; the asymmetric algorithm is often used to digital signatures and key transport, frequently-used algorithm is the rivest Shamir adelman (RSA); the diffie-hellman (DH) asymmetric key agreement algorithm is used to key agreement; and the SHA-1 and SHA-256 secure hash algorithms will be applied for integrality. Another significant asymmetric algorithm is known as elliptic curve cryptography (ECC), ECC can provide equal safety by use of shorter length key, the adoption of ECC has been slowed and maybe be encouraged recently.

To implement these cryptographic algorithms available resources are necessary such as processor speed and memory. So how to apply these cryptographic techniques to the IoT is not clear, we have to make more effort to further research to ensure that algorithms can be successfully implemented using of constrained memory and low-speed processor in the IoT.

VI. CONCLUSION

Application and principle of dynamic variable cipher security certificate is proposed in this paper. This protocol realized a “one time one cipher” method of communication based on key matrix. Both its encryption and decryption process are light weight. Timestamp technology used in communicating parties, which can guarantee their real-time. Through thetechnology of timeout, we can ensure its uniqueness ofthe communicating data, from what I have mentionedabove, we can see clearly that the dynamic

variablecipher security certificate is a very good application insensor layer in IOT.

REFERENCES

[1] Botta, Alessio, Walter de Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684-700.

[2] L Marin Marin, Leandro, MarcinPiotrPawlowski, and Antonio Jara. "Optimized ECC implementation for secure communication between heterogeneous IoT devices." Sensors 15, no. 9 (2015): 21478-21499.

[3] D HEMALATHA HEMALATHA, D., and BANU E. AFREEN. "Development in RFID (Radio Frequency Identification) Technology in Internet of Things (IOT)." Development 4, no. 11 (2015).

[4] S SicariSicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.

[5] AAgarwal Whitmore, Andrew, AnuragAgarwal, and Li Da Xu. "The Internet of Things—A survey of topics and trends." Information Systems Frontiers 17, no. 2 (2015): 261-274.

[6] H ShafaghShafagh, Hossein. "Toward computing over encrypted data in IoT systems." XRDS: Crossroads, The ACM Magazine for Students 22, no. 2 (2015): 48-52.

[7] JM BohliBohli, Jens-Matthias, Roman Kurpatov, and Mischa Schmidt. "Selective decryption of outsourced IoT data." In Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, pp. 739-744. IEEE, 2015.

[8] J GranjalGranjal, Jorge, EdmundoMonteiro, and Jorge Sa Silva. "Security for the internet of things: a survey of existing protocols and open research issues." Communications Surveys & Tutorials, IEEE 17, no. 3 (2015): 1294-1312.

[9] H ShafaghShafagh, Hossein, Anwar Hithnawi, Andreas Dröscher, Simon Duquennoy, and Wen Hu. "Poster: Towards Encrypted Query Processing for the Internet of Things." In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, pp. 251-253. ACM, 2015.

[10] W Shi Shi, Wenbo, Neeraj Kumar, Peng Gong, Naveen Chilamkurti, and Hangbae Chang. "On the security of a certificateless online/offline signcryption for Internet of Things." Peer-to-Peer Networking and Applications 8, no. 5 (2015): 881-885.

[11] A PatilPatil, Abhijit, GauravBansod, and Narayan Pisharoty. "Hybrid Lightweight and Robust Encryption Design for Security in IoT." (2015).

[12] HJ Kim Kim, HakJu, and Kwangjo Kim. "Toward an Inverse-free Lightweight Encryption Scheme for IoT." In 2014 Conference on Information Security & Cryptography. 2014.

[13] J PescatorePescatore, John, and G. Shpantzer. "Securing the Internet of Things Survey." SANS Institute, January (2014).

[14] Q Jing Jing, Qi, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and DechaoQiu. "Security of the internet of things: Perspectives and challenges." Wireless Networks 20, no. 8 (2014): 2481-2501.

[15] C TomaToma, Cristian, CristianCiurea, and Ion Ivan. "Authentication Issues for Sensors in IoT Solutions." In Proceedings of the 6th International Conference on Security for Information Technology and Communications (SECITC'13), pp. 2285-1798. 2013.

[16] Aggarwal, Charu C., Naveen Ashish, and Amit P. Sheth. "The Internet of Things: A Survey from the Data-Centric Perspective." (2013): 383-428.

[17] Xiaohui, Xu. "Study on security problems and key technologies of the internet of things." In Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on, pp. 407-410. IEEE, 2013.

[18] Altolini, Diego, VishwasLakkundi, Nicola Bui, Cristiano Tapparello, and Mattia Rossi. "Low power link layer security for iot: Implementation and performance analysis." In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, pp. 919-925. IEEE, 2013.