World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:5, 2017

Improving the Security of Internet of Things Using Encryption Algorithms

Amirhossein Safi

***Abstract*—**Internet of things (IOT) is a kind of advanced information technology which has drawn societies' attention. Sensors and stimulators are usually recognized as smart devices of our environment. Simultaneously, IOT security brings up new issues. Internet connection and possibility of interaction with smart devices cause those devices to involve more in human life. Therefore, safety is a fundamental requirement in designing IOT. IOT has three remarkable features: overall perception, reliable transmission, and intelligent processing. Because of IOT span, security of conveying data is an essential factor for system security. Hybrid encryption technique is a new model that can be used in IOT. This type of encryption generates strong security and low computation. In this paper, we have proposed a hybrid encryption algorithm which has been conducted in order to reduce safety risks and enhancing encryption's speed and less computational complexity. The purpose of this hybrid algorithm is information integrity, confidentiality, non-repudiation in data exchange for IOT. Eventually, the suggested encryption algorithm has been simulated by MATLAB software, and its speed and safety efficiency were evaluated in comparison with conventional encryption algorithm.

***Keywords*—**Internet of things, security, hybrid algorithm, privacy.

I. Introduction

IOT is a new network that is being used by wireless sensor connections and radio frequency identification (RFID) through wireless network and technology to achieve overall perception of information, reliable transmission, and intelligent processing. Hence, protecting privacy and safety are the essential features of IOT [1]. This security is related to tag information (RFID), wireless communications information security, network transmission of information security, privacy, and information processing security. Therefore, it is vital to have thorough study and research on design and improvement of security problems in IOT [2], [3]. IOT consists of three layers: sensing layer, transport layer and application layer. IOT has created a huge change in the medicine, household, business, industry, agriculture, and even nuclear reactors. The rapid development of security and privacy in large scale are the determinant factors of IOT. The main purpose of network security and information protection is to achieve confidentiality and integrity. Security issues are of great importance in enlarging the scale of network and devices [4], [5].

There are some security risks in both consumers and business in IOT, so data encryption can be used to reduce security risks [6]. Providing a suitable encryption algorithm can play an effective role in reducing the security risks. This kind of encryption can be a public key cryptography where high speed in encryption security and less memory requirement are its specifications [7], [8].

Amirhossein Safi is with the Department of Computer Engineering, Novin Hi-Tech Solutions,Tehran, Iran (e-mail: a-safi@agri-bank.com).

II. Related Works

In 2015 [9], a security model is presented based on SDN architecture. In the suggested model, both substructures, wired and wireless networks, have been used to provide safety. The proposed architecture is to create Ad-Hoc network and reticular objects such as sensors, tablet, smart phone, etc. One of the important features of SDN architecture is its ability to extend their security area to access the network.

In 2015, authors [10] provided a hybrid algorithm which has combined AES and ECC algorithms and has been applied in security of IOT.

In 2014 [11], a standard IP-based security framework has been offered for security solution in order to optimize IOT. This secure connection is based on the combination of end-to-end connection and public key cryptography.

In 2014 [12], a method is presented to resolve security challenges in IOT. In this method, first of all, the owner exports token related issues to access to the devices and connects to the token with oval ECDSA elliptically algorithm in order to prevent of exporter's security flaws.

In 2013 [13], a security framework is provided for IOT by SM2 encryption algorithm and resolving security problems between client and receptor in the information transmission process. That algorithm is carried out by using a wide range of IOT based on elliptically graph of ECC. This method is an innovative way to research on the security of IOT.

In 2013, authors [14] presented a systematic approach with four nodes containing individual node, process node, ecosystem technological node and smart thing node. In this method, security process needs responding required standards, strategies, policies, trends, and other documentations.

In 2012 [15], according to the security challenge of IOT, a security framework is presented based on 4G connection. This framework enhances the communication speed of IOT. Through this method, 4G client can access to wireless network resources.

A suggested method [16] in 2011 is presented for safe embedded security framework in IOT. This security framework is divided into hardware, software, and with highly light weight protocols in MAC layer and physical layer.

In 2014, authors [17] presented blowfish algorithm on FPGA by the use of VHDL programming language which had supervision on some of FPGA resources. Blowfish algorithm

has shown that it has good performance during the FPGA implementation and also is a good alternative for network security in IOT.

In 2014 [18], Hash encryption is presented with the aim of increasing security that was focusing on a smart home. In fact, the main purpose was security in IOT devices that can send messages with more security.

In 2013 [19], a system is proposed for IOT and security risks reduction in useful applications to equip management system which introduces a hybrid encryption algorithm based on DES and DSA encryption algorithms.

In 2013 [20], key technologies are presented with IOT such as RFID technology, electronic technology code identification, and ZigBee technologies. In this regard, key technologies framework and their usage in digital agriculture have been analyzed.

In 2013, authors [21] presented hybrid encryption algorithm based on DES and RSA encryptions in Bluetooth connections.

III. Proposed Method

Hybrid encryption technique is a new model that can be used in IOT. Hybrid encryption technique is for information integrity, confidentiality, being non-repudiation in data exchange for IOT. This paper analyzes hybrid encryption algorithm with the name of HAN. The suggested algorithm has special features in encryption and decryption in terms of speed even in building keys and it can also improve internet security by several structures during algorithm implementation and using digital signature. By default, tools and equipment for a smart home are considered as shown in the following flowchart.

Steps of a smart home cryptography are as follows:

- The user or the home resident has a public key that is generated by the symmetric encryption.
- Now messages and whatever which are needed to be encrypted will be sent to the asymmetric algorithm by the public key.
- Then, the message is encrypted by asymmetric encryption algorithm and will be sent to the receptor in the internet environment.
- Receptors (refrigerator, lamp, garage door, etc...) also own a private key that even the user or sender is unaware about it.
- Hackers cannot guess the passwords of tools and smart appliances because of the private key and it can enhance IOT system security in a smart home.
- Receptor attempts to decode a message from the sender by the private key and encrypted text. In this paper, we will present a new hybrid algorithm for secure access and increasing speed of building a key, encryption and decryption and finally less memory requirements in IOT by combining two algorithms of AES and NTRU [22].

A. Creating a Key

Key production process in AES is used to create a key. First of all, two 4 x 4 matrices, which are called stay and key, are used to produce key for encryption. We can choose a place from the state matrix and a key from the key matrix randomly and produce public key of H by sender in XOR operation.

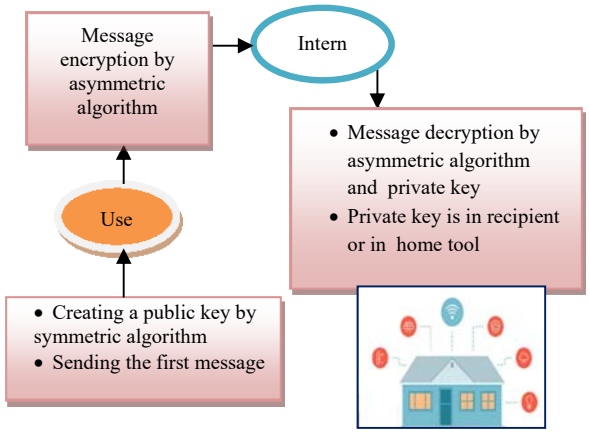

Fig. 1 HAN encryption algorithm usage in IOT

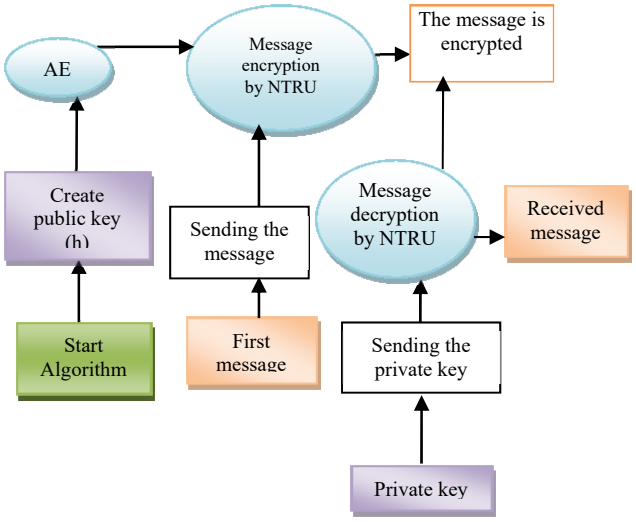

Fig. 2 HAN encryption algorithm steps sending public key

This step of HAN algorithm has been drawn from AEC algorithm. It should be noted that produced key of h is on the basis of hexadecimal. Then public key h is produced. The aim is sending a hidden message from sender to receiver in which private key is just recognized by the receiver and public key by both sender and receiver. So, encryption process must have a tight security. It means that the encrypted message by the sender will be sent to the receiver in secret and safety. Therefore, NTRU asymmetric encryption is used to enhance the security. When the sent message by the sender is encrypted, it should not be identifiable by any person other than intended recipient.

B. Encryption

Assume that a message is sent from the sender to the receiver. This message is in a multinomial called message. After making a multinomial message, the sender randomly chooses a multi nominal like r from the collection like Lr.

It should be noted that we can have a message by multi nominal r. So, it should not be revealed by the sender.

$$\text{Encryption} = \text{pr} \times \text{h} + \text{message} \quad (1)$$

This message will be transmitted to the receiver as an encryption message with security capability.

C. Decryption

When the message is encrypted, in other way receiver tries to open the message by its private key or to encrypt the message. For message decryption in HAN algorithm, NTRU algorithm will be used partially. The receiver has both private keys: f and fp. In fact, fp is conversed with multinomial of f, so it can be concluded that it will be $f * fp = 1$, and message receiver multiplies a message on the part of private key that is displayed below with the parameter a:

$$a = f \times \text{encryption} \quad (2)$$

$$a = f \times (\text{pr} \times h + \text{message}) \quad (3)$$

$$a = f \times \text{Pr} \times h + f \times \text{message} \quad (4)$$

To choose a correct parameter, coefficients of the polynomial formula between –q/2 and p/2 are selected. So as p = 3, then it drastically reduces and does not have any effect on the process, so we can conclude the following relation.

$$\text{pr} \times h = 0 \quad (5)$$

$$a = f \times \text{message} \quad (6)$$

In the next step, parameter b will be calculated. Just multiply private key f in initial message which has been sent by the sender.

$$a = b = f \times \text{message} \quad (7)$$

$$Decryption = \frac{(fp \times b)}{x^2} \quad (8)$$

Whenever Decryption = Message, we will be sure that the message will reach security to the recipient without any disorder.

D. Digital Signature

It would be better to use digital signature in provided HAN hybrid encryption algorithm to keep ID credit in this study. It is just for message validity and proof of identity and security. It should be noted that for digital signature, we must go from the sender to the receiver, so the receiver of the former step acts as the sender now, and the sender of the former step acts as the receiver.

$$\text{Encryptionsign} = \frac{(\text{message} \times f)}{x^2} \quad (9)$$

$$\text{Decryption} = \frac{\frac{h}{2} \times fp \times \text{Encryptionsign}}{2} \times h \quad (10)$$

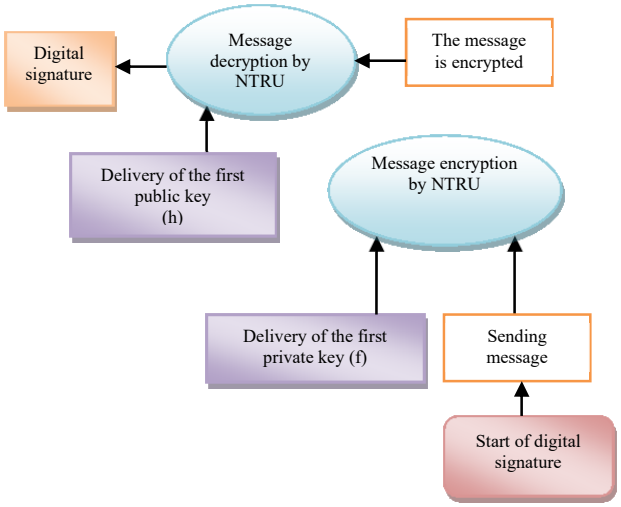

Fig. 3 Digital signature steps

E. Simulation and Evaluation

HAN algorithm has been simulated by MATLAB software, so it is compared with two algorithms of AES and RSA to check high speed of the algorithm in encryption process. The results are given in Table I.

TABLE I
THE TOTAL SPEED TIME OF HAN ALGORITHM IN COMPARISON WITH TWO OTHER ENCRYPTION ALGORITHMS

Algorithm	*HAN*	*AES*	*RSA*
Period of time for implementing the whole algorithm per second	0.321081	2.718182	2.350752

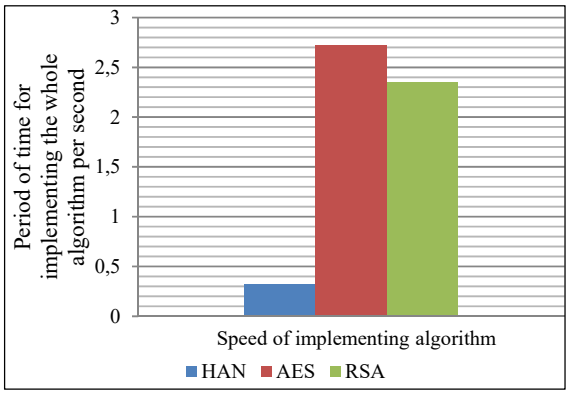

Fig. 4 Comparing the speed of implementing HAN algorithm with two other encryption algorithms

Digital signature is brought up to check security improvement in this algorithm, and finally, speed of digital signature has been compared with two other algorithms that had not applied digital signature. The results show that the speed of suggested algorithm even with digital signature is higher than the two others, and that is why algorithm is functional.

TABLE II
IMPLEMENTATION TIME OF DIGITAL SIGNATURE IN SUGGESTED ALGORITHM

ALGORITHM	Total time algorithm implementation (sec)
HAN by digital sign	0.58
AES without digital sign	2.718182
RSA without digital sign	2.350752

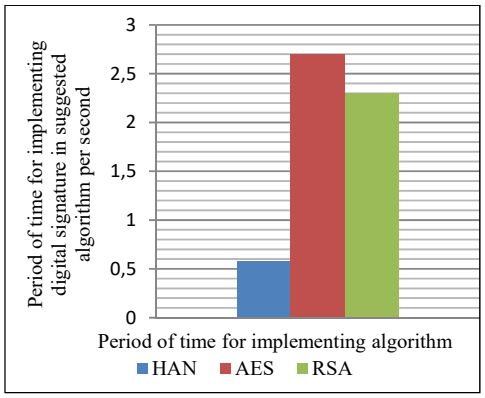

Fig. 5 Comparing period of time for implementing suggested algorithm considering digital signature with the other two algorithms excluding digital signature

IV. CONCLUSION

In this paper, we have discussed IOT, introduction and its usage, models, methods and security frameworks and also encryption algorithm in connection with IOT that researchers have studied before. Also, we have studied the suggested method in hybrid encryption algorithm used in IOT. We have provided a suggested method that can improve IOT by hybrid encryption algorithm. HAN algorithm is considered as a suggested method that is a combination of AES symmetric encryption algorithm and NTRU asymmetric encryption algorithm for IOT improvement. This algorithm has high speed to create a key, encryption and decryption, and acceptable security in IOT. Safety of this algorithm is due to multinomial usage in encryption, decryption and digital signature to achieve a correct message. This algorithm uses less memory because of less fiscal complexity. This algorithm makes available the encryption in IOT with deduced attacks and improved security.

REFERENCES

[1] W. Bruce D, GR. Milne, Y. G. Andonova, and F M. Hajjat. "Internet of Things: Convenience vs. privacy and secrecy." Business Horizons 58, no.6, Science Direct, pp. 615-624, 2015.
[2] R. Davice, "The Internet of Things Opportunties and challeng", European, p.p.1-8, 2015.
[3] G. Price, "The Internet of Things 2015", State of THE Market: Internet of Things 2015, Verison wireless company p. p1-24, 2015.
[4] X. Xingmei, Zh. Jing, W. He, "Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things", 3rd International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, IEEE, p.p.825-828, 2013.
[5] Y. Challal, E. Natalizio, S. Sen, and A. Maria Vegni "Internet of Things security and privacy: Design methods and optimization", Add Hoc Network, vol.32, Science Direct, p.p1-2, 2015.
[6] Ch. Qiang, G. Quan, B. Yu, L. Yang, "Research on Security Issues of the Internet of Things", International Journal of Future Generation Communication and Networking (IJFGCN), vol.6, NO.6, IEEE, pp 1-10, 2013.
[7] R. Weber, "Internet of Things New security and privacy challenges", Computer and Low Security Review, vol.26, issue1, Science Direct, p.p. 23-30, 2010.
[8] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, A. Bouabdallah" A systemic approach for IoT security', International Conference on Distributed Computing in Sensor Systems (DCOSS), Cambridge, MA, IEEE, p.p.351-355, 2013.
[9] F. Olivier, G. Carlos, N. Florent "New Security Architecture for IoT Network", Procedia Computer Science, vol.52, Science Direct, p.p1028-1033, 2015.
[10] M. Xin, H. China "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System", International Conference on Cyber-Enabled Disributed Computing and Knowledge Discovery, Xian, IEEE, p.p.62-65, 2015.
[11] H. Shafagh, A. Hithnawi" Poster Abstract: Security Comes First, A Publickey Cryptography Framework for the Internet of Things', International Conference on Distributed Computing In Sensor Systems (DCOSS), Marina Del Rey, CA, IEEE, p.p.135-136, 2014
[12] A. F. Skarmeta, J. L. Hernandez, M. V. Moreno" A decentralized approach for Security and Privacy challenges in the Internet of Things", IEEE Word Forum on Internet of Things (WF-IOT), Seoul, IEEE, p.p.67-72, 2014.
[13] N. Hong, Z. Xuefeng, "A Security Framework for internet of thingsbased on SM2 cipher algorithm", Fifth International Conference on Computer Science and Network Technology, Shiyang, Hubia, China, IEEE, p.p13-16, 2013.
[14] R. Arbia, Ya. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah. "A systemic approach for IoT security." In 2013¬ IEEE International Conference on Distributed Computing in Sensor Systems, p.p. 351-355. IEEE, 2013.
[15] L. Yuan Zeng, "A Security Framework for Internet of Things Based on 4G communication,-2nd International Conference On computer Science And Network Technology, Chanchun, China, IEEE, p.p1715-1718, 2012.
[16] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, "Proposed embeded seurity framework for internet of things", 2nd International Conference on Information Theory and Aerospace & Elentronic Systems Technology, Chennai, IEEE, p.p.1-5, 2011.
[17] K. Nur Prasetyo ST, Y. Purwanto, and D. Darlis. "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA."In Information and Communication Technology (ICoICT), 2014 2nd International Conference, Bandung, p.p. 75-79. IEEE, 2014.
[18] SB. Vinayaga, M. Ramnath, M. Prasanth, and V. Sundaram. "Encryption and hash based security in Internet of Things." In Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference, Chennai, p.p. 1-6. IEEE, 2015.
[19] P. Xu, Li. Min, and He. Yu-Jie. "A hybrid encryption algorithm in the application of equipment information management based on Internet of things." In 3rd International Conference on Multimedia Technology (ICMT-13). Atlantis Press, 2013.
[20] X. Yi Chen, Zh. Gang Jin, "Research on Key Technology and Applications for Internet of Things", Physics Procedia, vol33, Science Direct, p.p 561-566, 2012.
[21] R. Wuling, and Zh. Miao. "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication." In Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on Sanya, p.p. 221-225. IEEE, 2010.
[22] R. Jha, A. Kumar saini, "A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement", International Conference on Communication Systems and Network Technologies, Katra, Jammu, IEEE, p.p.80-84, 2011.