An efficient method for security measurement in internet of things

[1]Sahil Narang, [2]Tarun Nalwa, [3]Tanupriya Choudhury, [4]Nirbhay Kashyap
[1,2,4]Amity University Uttar Pradesh, India, [3]Asst. Prof. Senior Grade, SCS, Virtualization Dept., University of Petroleum and Energy Studies Dehradun, India
[1]yocg141@gmail.com, [2]tarunnalwa@gmail.com, [3]tanupriya1986@gmail.com, [4]nkashyap@amity.edu

ABSTRACT-The Internet of Things (IoT) is an interconnection of day to day objects in a network that are provided with colossal intelligence level. It has increased the usage of Internet gigantically by integrating every object for interaction through embedded systems that ends up in an extremely dispersed network of devices communicating with humans as well as electronic devices that support web. IoT is exploding in size and complexity, connecting a huge universe of consumer, industrial, and digital services to the network. IoT is in need of an advanced prototype for security, which considers the security issues from a holistic perspective comprising the advanced users and their intercommunication with this technology. In this paper, the advantages and disadvantages of IoT have been analyzed and also how current approaches are ensuring fundamental and basic security requisites and securing intercommunication of IoT, along with the rolling changes and scope for work in this field in the coming future.

Keywords- Internet of things, Security, AES, HAN

I. INTRODUCTION

IoT is an interconnection of day to day objects in a network that are provided with colossal intelligence level. IoT has increased the usage of Internet gigantically by integrating every object for interaction through embedded systems that ends upin an extremely dispersed network of devices communicating with humans as well as electronic devices that support web.

IoT is a promising phenomenon which will improve the quality of our lives. In the recent past, IoT has been the center of attraction of researchers and practitioners from all over the world.IoT devices are capable of capturing data, storing and processing it. It can also visualize services, monitor and manage various devices. There are some five billion connected devices in the world today, according to Gartner. And 50 billion IoT endpoints are expected to populate the planet by the year 2020. Nearly 30 percent of businesses worldwide have at least limited IoT deployments, by Strategy Analytics' count. And IDC suggests that IoT will be a US$7 trillion industry by 2020.

IoT can boost corporate profits worldwide and lower costs by realizing new efficiencies and boost new revenues by supporting new business models. There is a need of an advanced prototype for security which considers the security issues from a holistic perspective comprising the advanced users and their intercommunication with this technology.

II. THREATS TO SECURITY IN INTERNET OF THINGS

Implementing IoT itself has challenges. That includes figuring out how to secure connected devices and networks, and the data they handle. IoT devices are more prone to security problems than traditional computers [1]. This is important because the more connections and connected devices you have, the greater the opportunity for bad actors to steal data, gain unauthorized control of assets, and even potentially threaten safety.IoT devices can send and receive information between the objects without human intervention. Most IoT devices transmit information to the cloud or a local network in unencrypted state. Web interface which is used has security vulnerabilities, and does not use encryption. the security is an essential element for deploying Wireless sensor networks(WSN) [12]. Recently the concept of trust-based mechanism was proposed in WSNs such as traditional cryptographic and authentication mechanisms.

Consider how cybercriminals can remotely control and bring down anything from a website to a back-end business system to a connected car to a power grid to implanted medical devices to a country's weapons arsenal. According to the CommLaw group, more than 100 million IoT devices were affected by malwares from June 2016 to November 2016.As Robert Westervelt, security research manager atIDC, recently commented: ―As industrial corporationspursue industrial IoT (IIoT), it's vital to grasp the new threats that may impact critical operations. Greater connectivity with operational

978-1-5386-2459-3/18/$31.00 ©2018 IEEE

technology exposes operational groups to the categories of attacks that IT groups are accustomed to seeing, however with even higher stakes.The concern for a cyberattack is no longer targeted on loss of knowledge, but safety and availability.Consider an energy utility as an example—cyberattacks might disrupt power supply for communities and potentially have impact to life and safety."

One challenge to securing these environments is that many IoT endpoint manufacturers simply have not built security into their products. That's in part because they know that people want inexpensive devices, and adding security to them adds cost. Also, the limited processing power of some endpoints restricts encryption, connected devices frequently have easily exploited vulnerabilities, like default passwords that never get changed, remote access backdoors meant for use by field service technicians, and weak authentication.Some device manufacturers take a stab at security by employing trusted boot capabilities, encrypting network traffic, or using Secure Shell (SSH). But if they and the organizations that buy them don't implement these measures in the right way, such efforts can be ineffective.

Another part of IoT security challenge is simply that IoT is new, and rooted in both the information technology and operational technology worlds. Yet IT and OT have traditionally been siloed. And there's no real precedent for how to bring them together. Additionally, some of the people involved in supporting IoT implementations may not be clear on the goals and requirements of those efforts. And they probably don't understand everything that goes into endpoint data management and analytics, and into IoT security [2].

III. SECURING THE INTERNET OF THINGS

Securing IoT starts before the pieces are even put in place. It begins during the equipment and software selection process. Clearly, it's important to select equipment and software with built-in security when feasible.. Organizations have to be sure to change the default usernames and passwords on their IoT devices. Those that are left unchanged can be easily identified by botnets that scan for known usernames and passwords. And if they hit the jackpot, your devices can come under their control. Businesses also need to update their IoT devices with the latest operating systems and patches. That will ensure that they're up to date with a variety of features, including thelatest security ones.The best-prepared businesses will have the right processes and tools in place to monitor and secure app and API access.Securing the network, of course, is also an important part of the IoT security puzzle. Connectivity is the linchpin of IoT services, and it's important to protect against such attacks as man-in-the middle hacks and session Hijacking, which can intercept communications between the device and the cloud application.

Device data should always be encrypted when it's being transported to guard against attacks.While IoT devices don't support such application-level encryption, the cellular industry addresses it by using Global System for Mobile Communications (GSM) standardized encryption between mobile networks. In this case, the network initiates an encrypted communication with a ciphering mode request, and the device uses ciphering keys and encryption algorithms on the SIM card to securely transmit and receive data. Because the keys are never exposed outside the SIM card and the true identity of the end device is never revealed, this solution is highly secure.

Network authentication, meanwhile, helps ensure that devices communicate only with the applications they should. That involves verifying and authorizing devices on both the network and applications within the network. And safeguarded private networks isolate and shield IoT device data from other parts of the Internet. This also protects the enterprise from exposure if device data is attacked.Businesses may be familiar with this idea from their use of virtual private networks, but VPNs aren't an affordable option for low-cost IoT devices. A better choice is using cellular customer access point names to extend a highly secure local area network from the enterprise data center across the mobile network to remote IoT devices. Businesses can then allocate private IP addresses and specify additional levels of authentication and authorization [11].

Security is top of mind in any IoT project discussion and planning. For end-to-end protection and visibility, security should be built into any IoT strategy and solution from the ground up, instead of bolted onto the converged network later as an afterthought. As part of its commitment to this approach, Cisco announced its IoT Threat Defense cybersecurity architecture at the 2017 IoT World Forum. This framework is an umbrella program that focuses on the security segmentation of OT and IT networks, visibility, remote access, and services.

IV. PROPOSED METHOD

Hybrid encryption technique is a model that can be used for information roubustness and confidentiality in data exchange for the Internet of Things. This paper analyses Hybrid Encryption Algorithm as HAN. It has special features in encryption and decryption in terms of speed and it can also improve internet security by several structures during its implementation [10].

Steps of a smart home cryptography are as follows:

1. The user or the home resident has a public key that is generated by the symmetric encryption.
2. The messages to be encrypted are sent to the asymmetric algorithm by the public key.
3. Then, the message is encrypted by asymmetric encryption algorithm and is sent to the receptor in the internet environment.
4. Receptors (refrigerator, lamp, garage door, etc...) also own a private key and the user or sender is unaware about it.
5. Because of the private key, the hackers cannot guess the passwords of tools and smart appliances. Hence the security of the internet of things is enhanced.

Advance encryption algorithm (AES) is 6 times faster than Data Encryption Standard (DES) algorithm which was developed by IBM. The general structure of AES is shown in fig.1.

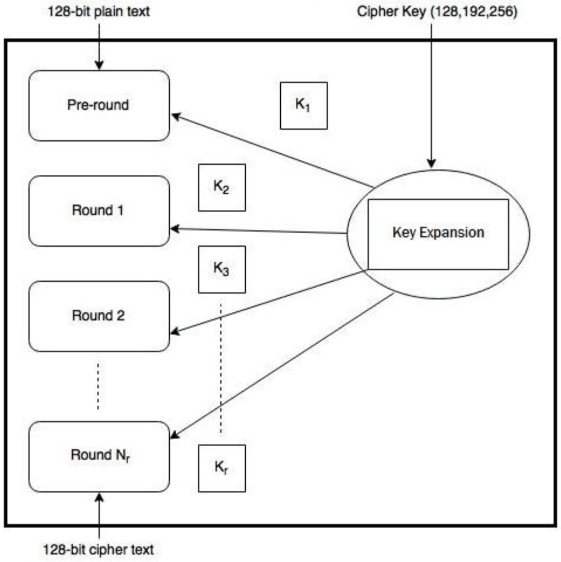

Fig. 1. General Structure of AES

This hybrid algorithm provides secure access and increases the speed of building a key. Also, the encryption and decryption and finally less memory requirements in Internet of Things by combining two algorithms of AES and NTRU.

A. The Process of Key Production

Key production process in AES is used to create a key. First of all, two 4x4 matrices. These matrices are used to produce encryption key and are known as stay and key.

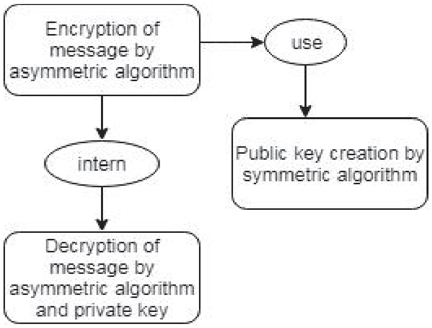
Encryption of message by asymmetric algorithm
use
intern
Public key creation by symmetric algorithm
Decryption of message by asymmetric algorithm and private key

Fig. 2. HAN encryption algorithm usage in IOT

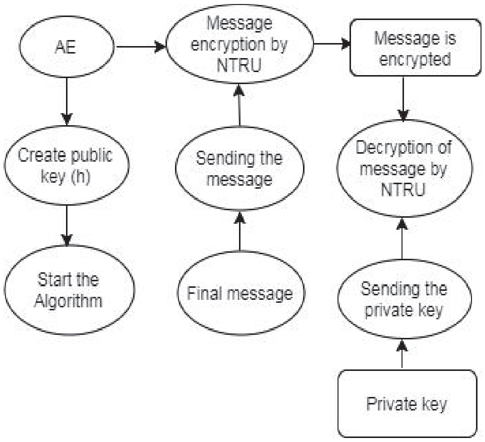

Fig. 3. HAN encryption algorithm steps sending public key

We can choose a place from the state matrix and a key from the key matrix randomly. The public key of H can be produced by sender by applying XOR operation.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. The hidden message in which private key is just recognized by the receiver and public key by both sender and receiver.The encryption process must be done secretly and safely [3].

B. Encryption of the message

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[7].

Encryption = pr x h + message …equation 1

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

C. Decryption of the messsage

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[9].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 x fp =1, and message receiver multiplies a message on the part of private key that is displayed below with the parameter a:

a = f x encryption …equation 2

a = f x (pr x h +message) …equation 3

a = f x Pr x h + f x message …equation 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.

pr x h = 0 …equation 5

a = f x message …equation 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 x message …equation 7

Decryption = (fb x b)/x^2 …equation 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 shouldbe 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[3].

Encryptionsign = (message x f)/x^2 …equation 9

Decryption =(h/2 x fp x Encryptionsign)/2 x h ...equation 10

E. Simulation and Evaluation

HAN algorithm it is compared with the AES algorithm to check which of them has high speed of the implementation in encryption process.

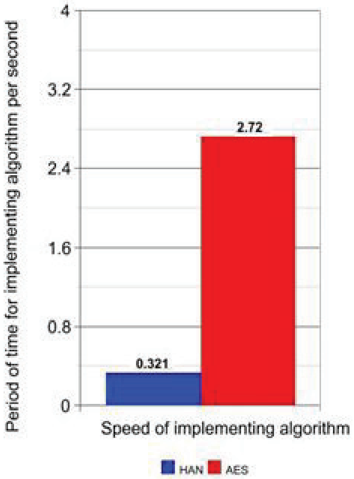

Fig.4. Comparing the speed of implementing HAN algorithm with AES algorithm

V. CONCLUSION

In this paper, we have discussed the internet of things, its advantages, disadvantages, threats to security, methods and security frameworks. We have studied the hybrid encryption algorithm used in Internet of Things and have provided a 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 the Internet of Things. 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 suggested algorithm makes available the encryption in the Internet of Things with deduced attacks and improved security.

VI. REFERENCES

[1] Caiming Liu et al―ANovel Approach to IoT Security based on Immunology", Ninth International Conference on Computional Intelligence and Security, 2013.

[2] A. Riahi, Y. Challal et al" A systemic approach for IoT security', International Conference on Distributed Computing in Sensor Systems (DCOSS), Cambridge, MA, 2013.

[3] Amirhossein Safi" Improving the Security of Internet of Things Using Encryption Algorithms" International Journal of Computer and Information Engineering, 2017.

[4] 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.

[5] 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.

[6] S. Babar et al ―Prposed embedded seurity framework for internet of things", 2nd International Conference on Information Theory and Aerospace &Elentronic Systems Technology, Chennai, IEEE, p.p.1-5, 2011.

[7] 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.

[8] SB. Vinayaga et al "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.

[9] 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.

[10] 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.

[11] N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad, Identity, Authentication and Capability Based Access Control (IACAC) for the Internet of Things, Journal of Cyber Security and Mobility, Vol. 1, No. 4, p. 309-348., march 2013.

[12] H. C. Hsu, K. D. Chang, J. L. Chen, H. C. Chao, A Survey on Trust Management Mechanisms for Wireless Sensor Networks & Future Internet of Things, Journal of Electronic Science and Technology, vol. 9, no. 4, pp. 364–367, 2011.