© 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
National Conference on Advanced Research Trends in Information and Computing Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering, Ahmedabad, Gujarat, India In association with International Journal of Scientific Research in Science, Engineering and Technology

Proposed Cryptographic Approach for Securing IOT Device

D. M. Trivedi[1], Prof. T. J. Raval[2]

[1]Computer Department, L.D.College of Engineering, Gujarat Technological University, Gujarat, India
[2]Computer Department, L.D.College of Engineering, Gujarat Technological University, Gujarat, India

ABSTRACT

Internet of Things (IoT) connects sensing devices to the Internet for the purpose of exchanging information.The Internet of Things (IoT) shall be able to incorpo-rate transparently and seamlessly a large number of different and heterogeneous end systems,hence the security is most important factor of this system as the system will be useful in healthcare, industry etc. in this paper we are going to provide information about security and cryptographic algorithm that are best suited for IOT.

Keywords:

I. INTRODUCTION

The Internet of Things(IOT) is a interconnected physical devices through internet. physical devices include car,machine,person smartphone and other items embedded with electronics , sensor, actuators,software and network connectivity on it. signals are collected by the sensor and transmitted to the network.

1.1 Architecture of IOT

From the perspective of architecture, the Internet of things can be generally divided into three layers, namely perception layer, network layer, and application layer. The perception layer transforms the information of things to the readable digital signals via RFID, sensors, etc.

On the other hand, the network layer transmits these digital signals to corresponding platforms via a connected network. In the end, the application layer unscrambles and applies digital signals through corresponding software.

Application layer provide end- to end communication between node.as shown in the figure 1.

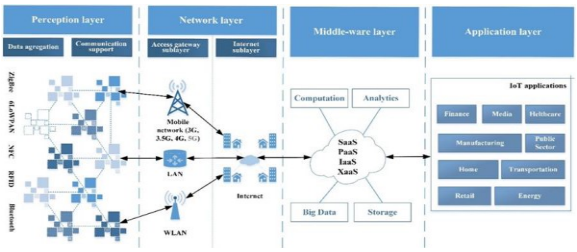


Figure 1. Architecture of IOT [16,17]

1.2 Need Of Security in IOT

Among these three layers, security is a problem to ensure signal is corrected collected, transmitted, and interpreted by the applications. Both the ordinary nodes and sink nodes are vulnerable to a variety of security attacks, such as denial of service attacks, or illegal control and failure. These attacks could compromise the sensitive information and result in malfunctions.

1.3 Types Of Attack on IOT

- ✓ Physical Attacks
- ✓ Side Channel attacks
- ✓ Cryptanalysis attacks
- ✓ Software Attacks
- ✓ Network Attacks

II. CRYPTOGRAPHIC ALGORITHM

There are various cryptographic algorithm available based on key distribution conventional cryptography is referred to as Conventional cryptography is referred to as symmetric encryption or single key encryption. Same key is used for encryption and decryption. This means that the encryption key is equal to the decryption key. Figure represents the simplified model for conversional encryption technique. In general, there are two types of the symmetric ciphers, namely, stream ciphers and block ciphers.

Figure 2. Symmetric Encryption Technique [1]

III. PROPOSED METHODS

AES-GCM

In the AES-GCM, only the AES encryption is utilized with the input and the output blocks of 128 bits. However, based on the security requirements, the key size could be determined as AES-128 (with 10 rounds), AES-192 (with 12 rounds), or AES-256 (with 14 rounds) [1]. In the AES encryption, all the rounds except for the last round have four transformations of SubBytes, ShiftRows, MixColumns, and AddRoundKey. For the last round, MixColumns is eliminated and only three transformations of SubBytes, ShiftRows, and AddRoundKey are used.

The transformation SubBytes (S-boxes) is implemented by 16 S-boxes. In the S-box, each byte of the input state is substituted by a new byte. In ShiftRows, the first row of the state remains intact and the four bytes of the last three rows of the input state are cyclically shifted. In the MixColumns transformation, each column is modified individually and in the final transformation, AddRoundKey, modulo-2 addition of the input state and the key of the corresponding round is performed [1].

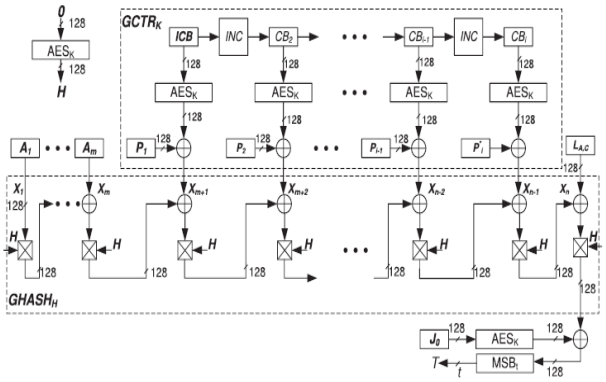


Figure 3. The GCM Authenticated Encryption Data Flow

NTRU :

NTRU (N-th degree Truncated polynomial Ring Unit) is an open source and patented public-key cryptosystem which uses lattice-based cryptography for encryption and decryption of files. The two keys used in this algorithm are: public key and private key. The key is used for the encryption is Public Key or to verify the digital signature but private key is used for decryption or to create digital signature

The Combination of AES-GCM, and NTRU will be used. it provides nonce misuse resistance, security over 256 bits and parallelizability. Stream ciphers take the plaintext as streams of characters with size of 1 bit or n-bit word. In cipher, the plaintext is encrypted (and decrypted) one character at a time. According to Alfred et al. [18], stream ciphers are used in real-time applications such as pay TV and communications. This is because they are able to run in high speed.

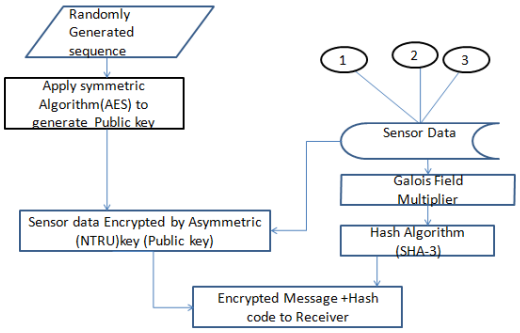


Figure 4. Proposed System Encryption Process.

Randomly generated Sequence has been applied to Symmetric algorithm AES and it will generate the public key, so the benefit of symmetric encryption has been achieved,the limitations of symmetric encryption has been overcome by encrypting the message with public key with NTRU algorithm.

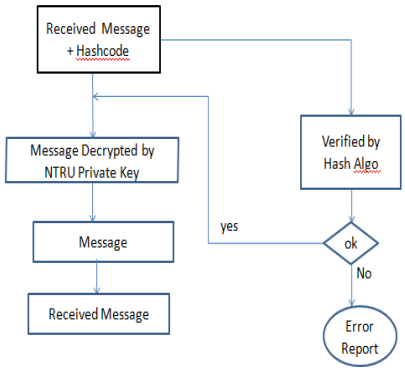


Figure 5. Proposed System for Decryption Process ecryption Process.

Encrypted message has been sent along with hash code to the receiver, the receiver will receive the message and first verify it by hash function output of hash function is the hash code in my proposed system hash code will be generated using sha-256, which is a non reversible function,if the verification function ouput is matched with the received code then decryption will be performed ,but if the verification output does not match withh received code then notification has been sent to the receiver.Decryption process is done with NTRU public key cryptographic algorithm and with private key of the user.

Table 1. Speed Time Of Han In Comparision With Two Other Encryption Algorithms

The Total Speed time of HAN in comparison with two other Encryption Algorithms			
Algorithm	HAN	AES	RSA
Period of time for implementing Whole algorithm per second	0,321081	2.718182	2.35072

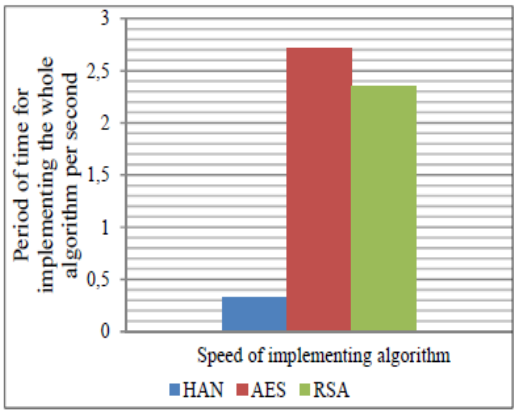
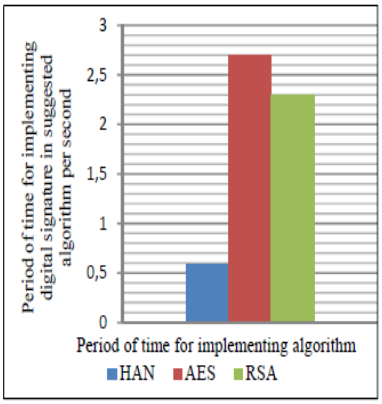


TABLE II
IMPLEMENTATION TIME OF DIGITAL SIGNATURE IN SUGGESTED ALGORITHM

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



IV. CONCLUSION

The Table 1 represents the speed of various algorithm according to that hybrid encryption algorithm will provide better and faster result. The proposed system will be capable enough to provide parallelizability, efficiency in security with authentication and confidentiality.

Table 2 represents the implementation time of various algorithm including hybrid encryption algorithm.which shows with digital signature also the proposed system generates good result.

Advantages of Proposed System:

- ✓ More efficient encryption and decryption in both hardware and software implementations;-
- ✓ much faster key generation allowing the use of “disposable" keys (because keys are computationally “cheap" to create).low memory use allows it to use in applications such as IOT Device.
- ✓ Here the combination of symmetric AES GCM and NTRU asymmetric algorithm is used, so the benefit of security and faster performance id achieved.
- ✓ AES-GCM is Authenticated Encryption algorithm,by using this we can reduce the time to create digital signature separately.

V. REFERENCES

[1]. markups.kdanmobile.com/sharings/

[2]. Joe Ruether, Cryptography Primer, http://jrruethe.github.io/blog/2014/10/25/cryptography-primer/

[3]. William Stallings, "Cryptography and Network Security: Principles & Practices", 4th edition, Prentice Hall.
[4]. Atul Kahate ,"Cryptography and Network Security:
[5]. Mingyuan Xin,2016 , "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission" International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery
[6]. T K Goyal," Lightweight Security Algorithm for Low Power IoT Devices, (ICACCI), Sept. 21-24, 2016
[7]. S. Singh, 2017,"Advanced lightweight encryption algorithms for IoT devices:survey, challenges and solutions",Springer-Verlag Berlin Heidelberg
[8]. A. Safi, 2017," Improving the Security of Internet of Things Using Encryption Algorithms", International Scholarly and Scientific Research & Innovation [5]2017 S Koteshwar,2016 "Comparative study of Authenticated Encryption" targeting lightweight IoT applications, 2168-2356 (c) 2016 IEEE,
[9]. Dr. S. S. Manikandasaran, 2016,"Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage" (IJCSITS),
[10]. M. Katagi," Lightweight Cryptography for the Internet of Things",
[11]. J Choi "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system"
[12]. A. SAJID, 2016,"Cloud-Assisted IoT-Based SCADA Systems", A Review of the State of the Art and Future Challenges, Digital Object Identifier
[13]. MIKAEL ASPLUND, 2016,"Attitudes and Perceptions of IoT Security in Critical Societal Services"Digital (IEEE) [11] Dieter Uckelmann,2011,"An Architectural Approach Towards the Future Internet of Things", DOI 10.1007/978-3-642-19157-2_1,Springer-Verlag Berlin Heidelberg 2011
[14]. A Tiwari, 2017,Challenges and Ongoing Researches for IOT (Internet of Things):
[15]. R Khan,2012,Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges,
[16]. Dr. S. Baskaran,Implementation of Enhanced Honey Encryption for IoT Security, International Journal of New Technology and Research (IJNTR)
[17]. I.Cvitic,2016, CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT DAAAM International,
[18]. M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, A Critical Analysis on the Security Concerns of Internet of Things (IoT), International Jurnal of Computer Applications,
[19]. L. Zheng, H. Zhang, W. Han, and X. Zhou, Technologies, Applications, and Governance in the Internet of Things, in: O. Vermesan and P. Friess (Eds.), Internet of Things - Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT, River Publishers, 2011, pp. 141–175.
[20]. S. Babar,2011,Proposed Embedded Security Framework for Internet of Things (IoT), 978-1-4577-0787-2/11/$26.00 2011 IEEE