TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

Modified Lightweight AES Based Two Level Security Model for Communication on IoT

*Binod Kumar Pattanayak[1], Seeven Amic[2]

1: Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India, Email: binodpattanayak@soa.ac.in

2: Faculty of Information and Communication Technology, Universite des Mascareignes, Mauritius, Email: samic@udm.ac.mu

**: Corresponding Author*

Article Info
Volume 82
Page Number: 2323 - 2330
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *18 January 2020*

Abstract

Security provisioning in an extremely heterogeneous environment like Internet of Things (IoT) has been a major challenge for the researchers and scientists around the globe. There are several approaches to network security and cryptographic algorithms entertain relatively higher popularity in the context of network security and inferably for IoT too. Furthermore, implementation of lightweight cryptography is mostly desirable for IoT security considering the fact that IoT encompasses huge number of resource constrained radio frequency driven small devices. In this paper, we have proposed an abstract secure communication model for IoT using lightweight symmetric block cipher AES where a two level security provisioning is implemented.

Keywords: *IoT, Security, Cryptography, Block Cipher, AES;*

1. Introduction

Global Internet has been one of the greatest innovations in the field of science and technology that has bound the people on the entire earth into a single communication platform. The diversified domain of applications has made it most popular over a few decades. However, current Internet is limited to human-to-human communication only. The further innovation of the Internet technology has resulted in emergence of a novel approach to communication called as Internet of Things (IoT) [Fig.1] that assumes device-to-device communications as well [1]. As revealed by experts, by the end of 2030, more than 30 billion devices are supposed to be connected to the backbone of Internet. Such devices may include small handheld mobile devices that are prone to attacks from external intruders [2]. Hence, a strong security mechanism must be devised to secure the communication of devices across IoT environment. In order to address the security of devices interconnected through IoT, it is essential to explore the characteristics of these devices such as confidentiality that refers to delivery of the data to the desired recipient, availability ensuring that the devices can receive the data when needed, integrity that ensures accuracy of data delivered, authentication by the receiver of data regarding its genuineness, heterogeneity that reveals the architectural diversity of interconnected devices that still conforms with IoT architecture as a whole and key encryption that ensures the secure communication among the devices where devices support a lightweight key management system [3]. Data security acquired by virtue of key management is the simplest definition of cryptography that refers to the process of

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

transformation of real world data into a unreadable as well as unrecognizable form in order to protect it from unauthorized access. IoT principally being a collection of huge number of small in dimension devices, energy constrained with limited storage and sensitive to external attacks, security of it necessitates implementation of lightweight cryptographic mechanisms for securing these devices.

Fig.1: Internet of Things (IoT) Architecture

2. Related Work

Implementation of cryptographic methods in order for addressing the security aspects of IoT devices has been a major attention of many researchers involved in exploring countermeasures to security vulnerabilities around IoT environment. A Quantum approach to IoT security provisioning is detailed in [4] wherein authors introduce a novel approach called Quantum IoT that is a combination of quantum computing and IoT. Here, authors rely on quantum mechanics law in order to address IoT security management. A hybrid security architecture is proposed along with an extra layer that represents the quantum state. This state is responsible for protecting IoT infrastructure from external attackers thereby protecting the security key making use of quantum cryptography BB84 protocol. This approach uses a classical cryptographic system named One Time Pad (OTP). Authors claim the successful implementation of the scheme for hybrid security management. Public key encryption algorithms like Elliptic Curve Cryptography (ECC) and RSA seem to be insecure enough for large-scale quantum computers as claimed by authors in [5]. Algorithms that are quantum resistant and lattice cryptography could be useful to overcome this issue. Nevertheless, implementation of lattice based cryptography on these high performance algorithms for IoT devices with limited resources would be challenging due to higher computational complexity of these algorithms. Authors have made an attempt to resolve this problem by devising a lattice based cryptography processor with configurable parameters. Light weight block ciphers can also be used to address security issues in IoT which has been rightly detailed in [6]. Cryptography and Steganography techniques can be useful to a larger extent in order to address IoT security issues in terms of data privacy and user authentication. Authors in [7] have introduced a security protocol called Elliptic Galois Cryptography protocol that successfully addresses these issues by virtue of encrypting confidential data obtained from various medical resources. Authors implement steganography in order to embed their already

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

encrypted data into an image of low complexity. Hidden thus data in the image are decrypted and recovered. Results justify the significance of this hybrid approach. Classical cryptographic algorithms that are considered to be heavy weight algorithms, are not suitable for resource constrained IoT devices. Again, modern cryptographic algorithms fall into two categories such as stream cipher and block cipher and stream cipher cannot handle long messages. Thus, block cipher based modern cryptographic algorithms can be useful for IoT devices that are resource constrained. Further, block cipher algorithms can be split into symmetric and asymmetric. Authors in

[8] propose a Hybrid Lightweight Algorithm (HLA) for addressing IoT security. In this algorithm, symmetric and asymmetric approaches can be used alternatively to provide security to resource constrained IoT devices. The symmetric cryptographic algorithms such as Advanced Encryption Standard (AES) operate with an assumption that the communicating end systems are secured and the encryption key is too stored securely. Nevertheless, IoT being a sufficiently vulnerable environment, the devices might be unprotected and the external attackers can still be able to access the memory of these devices, the data might be encrypted though. Thus, it is necessary that the key must be stored in such a way so as to make it difficult for the attacker to fetch it. As reported by authors in [9], white-box cryptography can be used for this purpose, but however, this may lead to additional adversaries resulting in security violations in devices. Authors propose an approach to overcome this issue wherein they implement white-box cryptography using Cipher Block Chaining (CBC) mode. Content-Centric Network (CCN) has been a recent innovation in data communication that aims at scalable content distribution across the devices on Internet. Authors in [10] claim that IoT environment being an open system of heterogeneous devices can function more efficiently, if it is implemented on CCN. Authors propose a secure IoT model that operates with CCN environment. Here, authors implement a public key that is certificate less and that can be used for resource constrained IoT devices. The proposed model relies on elliptic curve cryptography for security provisioning. A hyper elliptic curve based cryptography technique is demonstrated by authors in [11] that has been implemented for providing security in a IoT based healthcare system. A security architecture called DORBRI has been proposed by the authors in [12] for Department of Defense (DoD) that relies on Quantum key distribution which can be successfully used along with any existing cryptographic algorithm to provide secure communication. The end devices on IoT environment need that their performance parameters like computing speed, power consumption be optimized thereby maintaining a robust security level. ECC based algorithms can provide such a security feature as it has been observed in the literature. Authors in [13] have proposed a novel ECC processor architecture for IoT security provisioning. In order to provide security to small portable smart IoT devices, an integrated approach is proposed by the authors in [14] where authors integrate two cryptographic approaches such as blowfish cryptography and TBF-transposition. Here, blowfish block cipher is applied to the transposition of a plain text that ensures secure communication for portable smart devices. Handling security of text data exchanged over IoT environment holds the same significance as any other critical sensitive data. Current cryptographic algorithms are used to secure ASCII text. Authors in [15] propose a security solution for UNICODE text. Here, authors use a key-dependent dynamic Substitution Box (S-Box) to secure UNICODE text. Authors carried out the experiment with Python language and observed the improved security level of their proposed approach. Most of the wireless mobile IoT devices operate with Radio Frequency Identification (RFID) technologies that are prone to higher level of security threats and vulnerabilities. A set of solutions to it has been reviewed by authors in [16] where authors also discuss about some robust cryptographic protocol based

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

solutions for security provisioning of RFID technology.
[9]

3. Lightweight Cryptography

Most of the devices connected to IoT environment are small, mobile and operating on radio frequency smart devices with limited storage. Furthermore, these devices are significantly prone to external attacks and require robust security measures in order to support secure communication. Most of the existing cryptographic algorithms that are used for network security seem to be heavyweight algorithms in terms of storage requirement. Hence, such algorithms cannot be useful to provide security to resource constrained devices. Thus, lightweight cryptographic algorithms can only be compatible with smart IoT devices. The low level cryptographic algorithms fall into two separate categories such as Symmetric key cryptography and Asymmetric key cryptography [3].

Symmetric Key Cryptography

In symmetric key cryptography, both sender and the receiver share the same secret key for encryption and decryption respectively. Thus, it is also known as shared key cryptography. Such algorithms can be extremely useful for IoT devices for the reason that it operates fast thereby relying on XOR and permutation operations only. Implementation of these algorithms has two variations: stream ciphers and block ciphers. With stream ciphers, the key has exactly the same length as that of the data to be encrypted which is obtained from the plain text by applying bit by bit operation. In block cipher implementation, the cipher has fixed length that is obtained through various transformations using the symmetric key. Block ciphers can be very useful for resource constrained IoT devices.

Asymmetric Key Cryptography

In asymmetric key cryptography, a public key and a private key is used. It is also known as public key cryptography. Asymmetric key implementation of lightweight cryptography operates on a sufficiently complex algorithm and it is a time consuming procedure. Thus, these algorithms may not be useful for resource constrained smart IoT devices.

4. Modified Lightweight Advanced Encryption Standard (AES) for IoT Security

IoT encompasses heterogeneous devices where different devices may need different levels of security and each level may be associated with a particular key size. Advanced Encryption Standard (AES) represents a heavyweight block cipher which has three different sizes of key (128-bit, 192-bit and 256-bit) and thus, it is capable of providing multiple levels of security. However, a heavyweight AES cannot be used for resource constrained devices. A modified lightweight version of AES is proposed in [17] which can be successfully used for resource constrained RFID devices on IoT. The encryption process in AES is iteratively implemented in several rounds and each round is conducted in four different steps such as Subbytes, ShiftRows, MixColumns and AddRoundKey. As claimed by the authors, AES128 can be designed in a reource constrained version that significantly reduces the latency and thus can be compatible with the RFID IoT devices.

5. Modified Lightweight AES Based Secure Communication Model for IoT

As illustrated in the previous section, Modified Lightweight AES can be an optimal solution to ensure secure communication for IoT devices. It can be achieved in three phases: key generation, connection establishment, data transfer and connection termination.

Key Generation:

AES 128 encrypts and decrypts data blocks iteratively in 10 rounds using a 128- bit cryptographic key (16 Bytes). In each round, a different generated round key is XORed with the

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

state (data block). The round key is obtained from the original key through a process known as key expansion depicted in Fig.2. The key (K_0,.....,K_{15}) is converted into 44 words (W_4,. ,W_{47}) where each word is of 4 bytes.

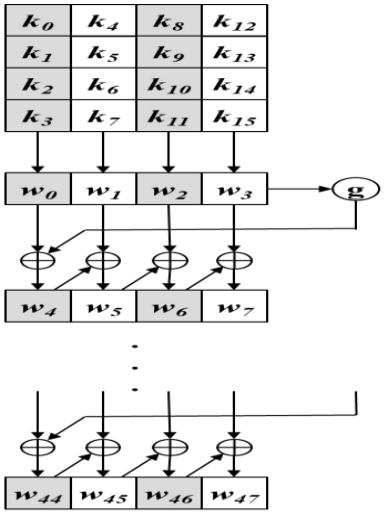

Fig.2: Key Expansion Algorithm

The function g is shown in Fig.3. A word w consisting of 4 bytes is first left-rotated followed by a substitution on each byte based on the S-table. The result is then XORed with a round constant RC_J, to produce the resulting word w'. The round constant is a word whose last three bytes are zeroes. The first byte of RC_1 is o1, that of RC_2 is 02 and so on, each round doubling the value of the first byte (in hexadecimal format). The values of the round constant are given in Table 1.

Table 1: The Round Constant Table

j	1	2	3	4	5	6	7	8	9	10
RC_j	01	02	04	08	10	20	40	80	1B	36

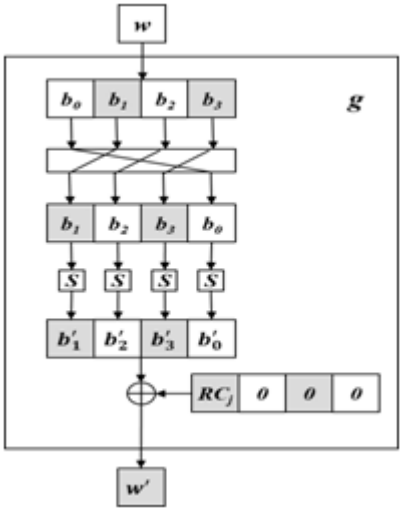

Fig.3: The g Function

The pseudocode of key expansion is given below.

KeyExpansion(byte key[16], word[44])

{

word temp

FOR i ← 0 **TO** 3

w[i] ← (key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])

ENDFOR

FOR i ← 4 **TO** 43

temp ← w[i−1]

IF i mod 4 = 0

temp ← g(temp)

ENDIF

w[i] ← w[i−4] ⊕ temp

ENDFOR

}

For example, given the original AES128 key for encryption

FC19F0FEFC1C9919C0CF689846821D6D,

the resulting round keys generated according to the key schedule described above is shown in Table 2.

Table 2: *Key Schedule Example*

Round	Round Key
1	FC19F0FEFC1C9919C0CF689846821D6D
2	EEBDCCA412A155BDD26E3D2594EC2048
3	220A9E8630ABCB3BE2C5F61E7629D656
4	83FC2FBEB357E4855192129B27BBC4CD
5	61E09272D2B776F78325646CA49EA0A1
6	7A00A03BA8B7D6CC2B92B2A08F0C1201
7	A4C9DC480C7E0A8427ECB824A8E0AA25
8	0565E38A091BE90E2EF7512A8617FB0F
9	756A95CE7C717CC052862DEAD491D6E5
10	EF9C4C8693ED3046C16B1DAC15FACB49

The AES key expansion algorithm was developed such that AES would be resistant to known cryptanalytic attacks. The following specific design criteria were considered as detailed by authors in [18].

1. Memory efficiency;
2. Fast on a wide range of processors;
3. Non symmetric and non linear;
4. High diffusion;

The properties of the key generation schema account for the high strength of the AES algorithm. However, there is still room for improvement of AES for lightweight cryptography. In [19], the authors propose a new approach for AES key schedule which provides very strong avalanche effect as early as the first round.

After the key generation process is completed, the process of secure IoT communication follows the steps as depicted in Fig.4.

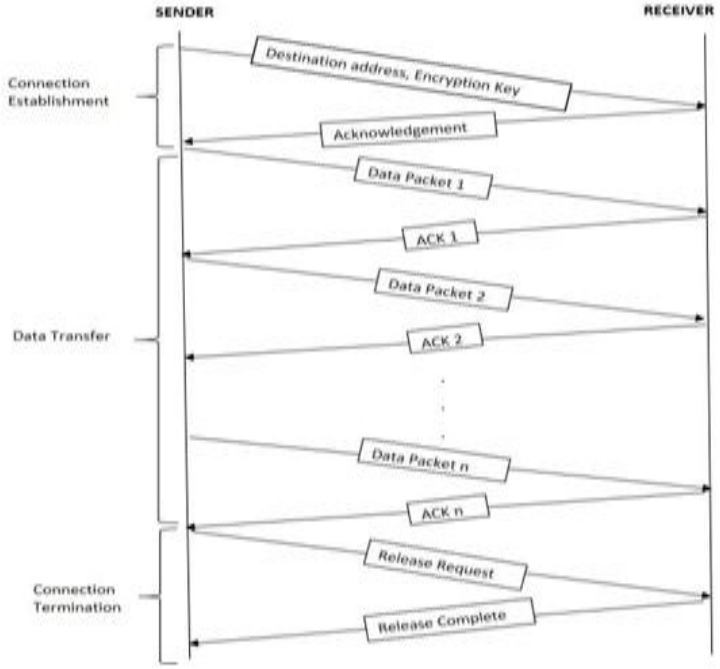

Fig.4: Two Level Secure IoT Communication

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

Connection Establishment: Before the data transfer between communicatiing nodes begins, the nodes must exchange with the encryption key. The sender places the encryption key into a control packet, adds the destination node address and sends it to the receiver using source routing. Here, by source routing we mean that the sender must have stored in its cache the shortest route to the desired destination node prior to the communication is initiated. The destination node on receiving this control packet, caches the encryption key and acknowledes back to the sender about the receipt of the encryption key using another control packet. Here, we assume that exchange of encryption key between the communicating nodes using a control packet has a strong authentication mechanism meaning that the only node whose address matches with the destination address incorporated in the control packet can be able to open the control packet. After the sender receives the acknowledgement from the receiver, the connection has been established and data transfer can begin. It should be noted that once the receiving nodes receives the encryption key from the sender, it caches it so that it can be further used for future communications with the same sender. And the process of key exchange can be skipped thereby.

Data Transfer: As depicted in Fig.4, the sender can send the encrypted data to the receiver. The receiver on receiving the packet, opens the data packet, decrypts the data using the kay and then caches it. Then it sends an acknowledgement back to the sender. The sender after receiving the acknowledgement for the previous packet, sends the next data packet. This process continues until the last data packet is acknowledged by the receiver.

Connection Termination: After the data transfer is over, the session can be terminated.

After data transfer is completed, the sender sends a control packet RELEASE REQUEST to the receiver and the receiver on receiving it sends back to the sender a control packet RELEASE COMPLETE. When the sender receives the packet RELEASE COMPLETE, the session is terminated. However, the communicating nodes can cache the key for future use rather than generating the key for each session between the same sender- receiver pair.

6. Conclusion and Future Work

Internet of Things (IoT), mostly regarded as future Internet that assumes device- to-device communication independent of human intervention, has grown in popularity in recent years. More and more devices tend to join this environment every second. Heterogeneity of devices on IoT imposes significant challenges to secure these devices. Cryptographic approaches to network security have been used successfully over the years. Considering the fact that IoT may connect billions of small resource constrained radio frequency operated wireless mobile devices, implementation of lightweight cryptographic algorithms is desirable. Here, we propose an abstract secure IoT communication model using lightweight block cipher. In our further research in this direction, it would be interesting to investigate how far this model is practicable and to what level it can be competent to address the IoT security vulnerabilities.

7. Reference

[1] Ramlowat D. and Pattanayak B. K., Exploring Internet of Things (IoT) in Education: A Review, Advances in Intelligent Systems and Compuitng 863, pp.245-255, 2019.

[2] Hosenkhan R. and Pattanayak B. K., A Secured Communication Model for IoT, Advances in Intelligent Systems and Compuitng 863, pp.187-193, 2019.

[3] Dutta I. K., Ghosh B. and Bayoumi M., Lightweight Cryptography for Internet of Insecure Things: A Survey, Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp.475-481,

January - February 2020
ISSN: 0193 - 4120 Page No. 2323 - 2330

2019.

[4] Rahman M. S. and Haider M.H.E., Quantum IoT: A Quantum Approach in IoT Security Maintenance, Proceedings of the International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp.269-272, 2019.

[5] Banerjee U., Pathak A. and Chandrakasan A. P., An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things, Proceedings of IEEE International Solid-State Circuits Conference, 2019.

[6] Shin H., Lee H. K., Cha H. Y., Heo S. W. and Kim H., IoT Security Issues and Light Weight Block Cipher, Proceedings of the IEEE International Conference on Artificial Intelligence in Information and Communication (ICAIIC 2019), pp.381-384, 2019.

[7] Khari M., Garg A. K. and Gandomi A. H., Securing Internet of Things (IoT) Using Cryptography and Steganography techniques, IEEE Transactions on Systems, Man and Cybernetics Systems, 2019, (Accepted)

[8] Thapiyal S., Gupta H. and Khatri S. K., An Innovative Model for the Enhancement of IoT Device Using Lightweight Cryptography, Proceedings of the Amity International Conference on Artificial Intelligence (AICAI 2019), pp.887-892, 2019.

[9] Saha A. and Srinivasan S., White-box Cryptography Based Data Encryption-Decryption Scheme for IoT Environment, Proceedings of the 5th International Conference on Advanced Computing and Communication Systems (ICACCS), pp.637-641, 2019.

[10] Adhikari S. and Ray S., A Lightweight and Secure IoT Communication Framework in Content-Centric Network Using Elliptic Curve Cryptography, Recent Trends in Communication, Computing and Electronics, Lecture Notes in Electrical Engineering 524, pp.207-216, Springer, 2019.

[11] Kavitha S., Alphonse P. J. A. and Reddy Y. V., An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Healthcare System, Journal of Medical Systems, Vol.43, No.8, 2019.

[12] Dorothy B. A. and Britto S. R. K., DORBRI: An Architecture for the DoD Security Breaches Through Quantum IoT, Proceedings of the International Conference on Computer Networks and Communication Technologies, Lecture Notes on Data Engineering and Communications Technologies, pp.491-496, 2019.

[13] Kudithi T. and Sakthivel R., High-performance EEC Processor Architecture Design for IoT Security Applications, The Journal of Supercomputing, Vol.75, No.1, pp.447-474, Springer, 2019.

[14] Sharma S. K., Rao M. S., Rao L. P. C. and Chaitanya P., Integrated Cryptography for Internet of Things using TBF Approach, Emerging Research in Computing, Information, Communication and Applications, Advances in Intelligent Systems and Computing 882, pp.41-52, Springer, 2019.

[15] Maram B., Gnanasekar J. M., Manogaran G. and Balaanand M., Intelligent Security Algorithm for UNICODE Data Privacy and Security in IoT, Service Oriented Computing and Applications, Vol.13, No.1, pp.3-15, Springer, 2019.

[16] Khodjaeva M., Obaidat M. and Salane D., Mitigating Threats and Vulnerabilities of RFID in IoT Through Outsourcing Computations for Public Key Cryptography, Security, Privacy and Trust in the IoT Environment, pp.39-60, Springer, 2019.

[17] James M. and Kumar D.s., An Implementation of Modified Lightweight Advanced Encryption Standard in FPGA, Procedia Technology, Vol.25, pp.582-589, 2016.

[18] Daemen, J., Rijmen, V.: The Design of Rijndael. New York. 255 (2002). doi:10.1007/978-3-662-04722-4

[19] Pehlivanoğlu, M.K., Sakalli, M.T., Duru, N., Sakalli, F.B.: The New Approach of AES Key Schedule for Lightweight Block Ciphers. IOSR J. Comput. Eng. 19, 21–26 (2017). doi:10.9790/0661-1903042126