Indian Journal of Science and Technology, Vol 9(28), DOI: 10.17485/ijst/2016/v9i28/98382 , July 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Analysis of Lightweight Cryptographic Solutions for Internet of Things

Isha and Ashish Kr. Luhach*

Lovely Professional University, Jalandhar - 144411, Punjab, India; isha.batra2487@gmail.com, ashishluhach@acm.org

Abstract

Internet of Things (IoT) enables physical things to communicate, compute and take decisions based on any network activity. This calls for a secure solution for communication among heterogeneous devices. With the development in Information and Communication Technology (ICT), a unique impact of smart things is observed in our everyday life. IoT can consider users that interact in heterogeneous environment. In heterogeneous environment motive of each user in IoT can be different in form of communication and computation and is difficult to be judged. A malicious user can destroy the security and privacy of the network. This study gives a detailed analysis of existing security solutions for IoT. Firstly, a comparison of lightweight cryptography algorithms is made on basis of block size, key size, number of rounds, and probable attacks. Later, the various security issues in IoT are discussed along with possible solution. Security solutions in IoT will improve the trust over IoT. A secure solution that will require less computational power and is less vulnerable to existing attacks is desired.

Keywords: Internet of Things (IoT), Lightweight Algorithms, Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN)

1. Introduction

IoT is an emerging technology in this expanding era of smart things[1]. Smart things can be any physical objects like phone, laptop, refrigerator, AC, charger, and many more. IoT can be defined as a network of uniquely identifiable, accessible, and manageable smart things that are capable of communication, computation and ultimate decision making.

It is mentioned that things in IoT can be connected using wireless connections like RFID, Bluetooth, ZigBee, WSN, WLAN, WMAN or Wi-Fi[2]. The number of things or users connected to IoT is growing exponentially and around 2020 the number of connections may reach 50 billion. Hence, the bandwidth requirement of IoT will also increase exponentially. Licensed and unlicensed bands are available for communication. Licensed bands are paid and are used in applications like 2G, 3G and many more. Unlicensed frequency bands are reserved for industrial, scientific and medical applications also known as ISM bands. The existing ISM bands are 433 MHz, 915 MHz and 2.4 GHz. The ISM band used in IoT is 2.4 GHz for Wi-Fi enabled communication.

For the complete deployment of IoT different enabling technologies like RFID or sensors are required. As mentioned, RFID in IoT can be used to identify the things and track the current status of things in real time like its location[3]. RFID can be used in application like retail management, transport systems, security or inventory management. RFID use radio waves to identify the things uniquely through electronic barcodes. As described in[4], RFID is built on three components- RFID tag/transponder, RFID antennas and RFID reader which maintain the data on the microchip. According to[5], the two major components of RFID are RFID reader and RFID tag. RFID tag is attached to each and every thing which is active in the network. It comprises of a microchip that is punched with unique identity of a particular thing. RFID reader is used to access the information from the tag and pass on this information to the application system[6]. Another technology that can be used in IoT is sensors. Sensors can be used to connect the information environment to the physical

*Author for correspondence

environment in IoT. Wireless Sensor Network (WSN) is used to sense and collect information related to an activity in real environment[7] and that information is passed to the network for generating responses. The application areas of WSN are temperature control, humidity control, remote sensing, military any disaster management[7]. But WSN works only for collecting the data and is not able to process the data for final decision making. So, IoT took this advantage of WSN for collecting the data, and further apply processing on this data to take fruitful decisions[7]. IoT acts as an extension to WSN in aforementioned application areas and broaden them in more functional way[8].

The main objective of this research paper is to give an ideal view of challenges and security solutions for IoT. The paper is organized as follows: In Section 2, motivation to carry out this research work is mentioned. In Section 3, the related work on current lightweight algorithms in IoT for security is done. In Section 4, all the issues related to IoT are presented. Later, the review narrow downs to the most prominent issue in IoT, and its recommended solution.

2. Research Motivation

IoT help in creating connections between dissimilar things present in heterogeneous environment. This kind of openness and very less human intervention can make IoT exposed to number of attacks like man in middle attack, Denial of Service (DoS) attack. Moreover, any device can access the network that leads to unauthorized access. These attacks can damage device physically and network connections too. This will ultimately compromise the security and privacy of IoT. As, IoT are resource constrained with less power, bandwidth, less storage, so an efficient security solution is required that will not chomp through the resources of IoT.

3. Current Security Solutions in Iot: Related Work

IoT can use internet only for connecting and establishing communication between things in the network. There is much more to further work upon in IoT like making decisions after communicating and that too in real time. So, architecture of internet cannot be directly employed for IoT.

In literature number of architectures was proposed for IoT. Authors in[9] mentioned that IoT have a three layered architecture. The three layers of IoT are perception layer, network layer and application layer from bottom to top. A 5 layered architecture was proposed in[10] composed of perception, transport, processing, application, and business layer.

With the increase in application requirements of the user a vast amount of data is shared among themselves. So, security and privacy of IoT is intricate than other networks as personal data of user is communicated like location, time, information. The security services required to be maintained in IoT so as to enhance the trust of users are

- **Confidentiality:** Data at rest or in transit is only accessible to the sender or receiver.
- **Integrity:** While data is in transmission no intruder is able to modify the original contents of the data.
- **Authentication:** The identity of the sender should be verified to the receiver to judge the validity of data.
- **Authorization:** Only legitimate users are able to access the resources of the IoT and maintain connect among others.

Security architecture was proposed that will secure the data exchanged between business partners and assures above mentioned services[11]. A security and quality assuring architecture was also proposed in[12] but it still has a challenge to manage the open related data in IoT. As IoT comprise of heterogeneous connected things, a standard architecture is imposed on all the things with 4 layers. Each layer will provide an inbuilt security protocol that will help to achieve security services before transmitting data from one layer to other.

4. Security Architecture of IoT

- **Physical/Perception Layer:** It is the bottom layer of IoT that is combination of physical and MAC layer in internet architecture. It is used to collect the information using RFID, sensors, or GPRS. IEEE 802.15.4 is used as a standard specification at this layer for IoT. IEEE 802.15.4 works for low cost, battery operated things[13]. IEEE 802.15.4 security solution is available at this layer which is still vulnerable to attacks.
- **Network Layer:** Physical layer transmits collected information to network layer. Network layer is used to divide the message to packets and to route the packets from source to destination by using the IPv6 addressing mechanism. As number of connected things in

IoT is expanding so IPv4 address space is replaced by IPv6 having more address space. Inbuilt cryptography protocols like AES, DES can be implemented by using IPSec at network layer.

- **Transport Layer:** IoT uses User Datagram Protocol (UDP) for end to end communication. As UDP is an unreliable protocol so a security mechanism using DTLS is incorporated at this layer.
- **Application Layer:** The actual deployment of intelligence of IoT is understood at this layer. It can be used in number of applications like retail, social activity, health, or for personal use. Constrained Application Protocol (CoAP) is used on this layer for the constrained IoT devices.

The existing protocol at each layer, along with security protocol and attacks at each layer is summarized shown in Table 1.

CoAP was earlier using the security of IPSec and DTLS. The predefined security mechanisms are vulnerable to aforementioned attacks. So, cryptography algorithms can be incorporated in them. Cryptography algorithms can be symmetric and asymmetric.

Symmetric algorithm uses a single private key for communication. Sender and receiver share same key for communication. Symmetric key assures confidentiality and integrity of data, but do not guarantee authentication. Advantage of symmetric is less number of keys required with less key size. Disadvantage is secure key distribution among both the parties, and it does not authenticate the sender. Traditional Symmetric algorithms AES, DES, Triple DES, Blowfish, IDEA are compared on the basis of their properties like data size, key size, number of rounds, structure and existing attacks shown in Table 2.

Asymmetric uses pair of public and private key for communication. Asymmetric assures confidentiality, integrity, and authentication. For confidentiality and integrity sender encrypts the data using public key of receiver that can be only decrypted by private key of receiver. To assure authentication, data is encrypted by private key of sender and receiver confirms it by decrypting it with public key of sender. Advantage of Asymmetric cryptography is it supports all security services, but disadvantage is the large size of key which will increase the complexity of algorithm. The most common algorithms used are RSA by Rivest, Shamir and Adleman, Deffie Helmen key exchange (DH), Elliptic Curve Cryptography (ECC), and Hash functions.

Traditional Symmetric and Asymmetric algorithms are not apt for IoT environment due to the limited power

Table 1. Security protocols in IoT

Layer	Protocol Used	Security Protocol	Attacks
Application	COAP	Not fixed designed by user	Depend on Protocol
Transport	UDP	DTLS	Attack on RC4, DoS Attack
Network	IPv6, RPL	IPSec	DoS Attack
Perception	IEEE 802.15.4 PHY, MAC	IEEE 802.15.4 security	DoS, Attack on authentication, integrity

Table 2. Comparison of existing symmetric cryptographic algorithms

Algorithm	Data Size	Key Size	No of Rounds	Structure	Possible Attacks
AES	128 Bits	128/192/256	10/12/14	Feistel	Not any
DES	64 Bits	56	16	Feistel	Brute force
Triple DES	64 Bits	168	48	Feistel	Meet in middle
Blowfish	64 Bits	128-448	16	Feistel	Second order differential
IDEA	64 Bits	128	8	Substitution-Permutation	Related key
TEA	64 Bits	128	64	Feistel	Related key

devices, low computational resources, and less memory capacity of IoT. So, lightweight security algorithms were proposed for IoT. Lightweight solutions are light in terms of their key size, memory requirements and execution time so that fewer resources will be utilized as compared to heavy weight solutions.

5. Symmetric Lightweight Algorithms FOR IoT

- **Advanced Encryption Standard (AES):** AES is used as an inbuilt solution in COAP at application layer. It is a symmetric block cipher standardized by NIST. It uses substitution permutation network and works on 4*4 matrix having block length of 128 bits. Every byte gets affected by subbytes, shiftrows, MixedColumns, AddRoundKey[14]. Key size than can be used is 128, 192, 256 bits. AES is still vulnerable to man-in-middle attack[15].
- **High security and lightweight (HIGHT):** Hight uses very basic operations like addition mod 2^8 or XOR to work for Feistel network. It has a block size of 64 bits, work in 32 rounds on128 bit keys[16]. Its keys are generated while encryption and decryption phase. A parallel implementation of higth was proposed in[17] that requires less power, mentioned in few lines of code, and improves speed for RFID systems. Higth is vulnerable to saturation attack.
- **Tiny Encryption Algorithm (TEA):** TEA is used for constrained environments like sensor networks or smart things. It is written in very few lines of code. It does not use a complex program but requires simple operations of XOR, adding and shifting. It uses a block size of 64 bits and 128 bit keys and does not make use of existing tables or any predefined computations[18]. Number of variants exists for TEA like extended TEA[19], Block TEA and so on. These extensions try to resolve the problems in original TEA like equivalent keys. But still due to its simple operations TEA and its variant are susceptible to number of attacks.
- **PRESENT:** It is based on SPN and is used as ultra lightweight algorithm for security. It works on substitution layer uses 4-bit input and output S-boxes for hardware optimization. It has key size of 80 or 128 bits and operates on 64-bit blocks[20]. PRESENT has been presented as a lightweight cryptography solution in ISO/IEC 29192-2:2012 "Lightweight Cryptography"[21]. PRESENT is vulnerable to differential attack on 26 out of the 31 rounds[22].
- **RC5:** It was first coined by Rivest for rotations that are data independent[23]. It posses Feistel structure and can work well as lightweight algorithm as it is used in wireless sensor scenarios. RC5 is considered as w/r/b, where w refers to word size, r stands for number of working rounds, and b will tell about the number of bytes in encryption key. RC5 generally works on 32 bit size but its variants can be 16, 32, 64. It can work for 0, 1, .., 255 rounds using 0,1,..255 key bytes. Standard key size is 16 byte on 20 rounds of operation. RC5 is vulnerable to differential attack[24].
- Based on literature review conducted, comparison of all aforementioned symmetric lightweight algorithms is made on the basis of code length, structure, number of rounds, key size, block size and attacks shown in Table

Table 3. Comparison of symmetric lightweight cryptography algorithms in IoT

Symmetric Algorithm	Code length	Structure	Number of rounds	Key Size	Block Size	Possible Attacks
AES	2606	SPN	10	128	128	Man-in-middle attack
Hight	5672	GFS	32	128	64	Saturation attack
TEA	1140	Feistel	32	128	64	Related Key Attack
PRESENT	936	SPN	32	80	64	Differential attack
RC5	Not foxed	ARX	20	16	32	Differential attack

6. Asymmetric Lightweight Algorithms for IoT

- **RSA:** It was invented by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman in 1978. RSA works on generating public and private key pair by selecting two large prime numbers[25]. Find their modulus and choosing at random their encryption key and thus calculating the decryption key. Public key is published openly whereas private key is made secure[26]. A more secure RSA encryption is proposed in[27] that is used to encrypt and decrypt files for maintaining privacy of user.
- **Elliptic Curve Cryptography (ECC):** It requires less key size as compared to RSA. Hence it has fast processing and less storage requirements. It was invented by[28]. It s built on algebraic system where it takes two points on elliptic curve. Discrete logarithm problem is used to generate key that is used to compute key. In[29] a secure hardware implementation on ECC is proposed for small areas that will lead to faster computations in real time. ECC is optimized for 6LoWPAN nodes by working on its complex multiplication operation. Rather than using microprocessors operation for multiplication, bit shifting is used in[30] to optimize the use for low power devices.

7. Attacks on Existing Algorithms

Existing security solutions in IoT are still vulnerable to following attacks:

- Denial of Service (DoS): It will halt the services of network for the authorized users due to access of network connection requests from unauthorized users.
- Man-in-Middle: In this an intermediary user is able to get the key of one of the sides and will start communication as if it is the valid party.
- Eavesdropping: Intruder is able to listen the communication between sender and receiver. So this is attack on confidentiality.
- Masquerading: An intruder possess the identity of any other authorized user. So it can tear down the resources of IoT.
- Saturation: In this intruder will try to use the physical and mental ability of authorized party by its immense use.
- Differential: Change in input behavior will affect the output. So this attack is able to find the key from network transformations.

8. Research Challenges in IoT

This study reveals number of challenges allied to IoT.

- Lack of human intervention may lead to physical as well as logical attacks.
- IoT uses wireless communication that is vulnerable to number of attacks like eavesdropping, man-in-middle, Denial of Service (DoS) and many more.
- Any device can connect to the network so that may cause unauthorized access to the network.
- IoT devices are resource constrained in terms of power and bandwidth so exercising intricate security solutions can hinder the efficient working of devices.

So challenges can be things related or network related. Challenges concerning things are power limitation, heterogeneous platforms, and security and privacy. Network related issues are scalability, bandwidth issues, and security and privacy.

9. Research Problem

Now-a-days IoT is admitting in homes, work places, social places or in business firms that will open doors for security and privacy challenges. So, security and privacy issues are becoming major reasons of concern in operation of IoT. The amount of loss that can occur is prominent to imagine if any attack is injected in IoT. Various attacks on IoT exist like eavesdropping, spoofing, Denial of Service (DoS), replay attacks, false signals injection. These attacks will tear down the security services of IoT like confidentiality, integrity, and authentication; moreover, it will impact the privacy of users. IoT provides inbuilt primitive security solutions at each layer, which are still vulnerable to attacks.

Traditional cryptography and authentication schemes do not fit well in IoT scenario due to its constrained resources like power, real time execution. So, lightweight cryptography solutions tend to work well in IoT. Number of lightweight Symmetric and Asymmetric cryptography algorithms exists in literature like AES, HIGHT, RC5, PRESENT, RSA, ECC and many more. These existing solutions do not guarantee an optimum level of security

in real time communication due to more execution time, code length, and memory requirements. Execution time includes time for key management and distribution, encryption and decryption that decides the effectiveness of the protocol. Asymmetric algorithms are slow due to their large key size, whereas symmetric algorithms can provide only confidentiality and integrity but no authentication leading to attack on availability. This can affect real time information collecting and processing and will fritter away the resources of IoT.

This calls for a secure algorithm for IoT that will guarantee services like confidentially, integrity and authentication in optimal time.

10. Proposed Idea

On the basis of literature survey carried out many researchers have proposed lightweight symmetric and asymmetric security algorithms for IoT. Symmetric algorithms provide confidentiality, integrity, have small key size, and are less complex but they do not offer authenticity and distribution of keys in them is a challenging task. On the other hand, asymmetric algorithms provide confidentiality, integrity, and authenticity, but their key size is too large which make them more complex and not apt for constrained IoT scenario. So, there is a need of secure algorithm that will map best features of lightweight symmetric and asymmetric algorithms in such a way that it will take less execution time with optimum energy requirements and will assure all security services like confidentiality, integrity and authenticity.

11. Conclusion

IoT faces number of challenges like power, bandwidth, scalability, heterogeneity, security and privacy. Security and privacy is the most imperative challenge to solve to maintain the trust of users in IoT. Pre defined security solutions at each layer are still susceptible to attacks. So cryptography algorithms can be used to assure security. But traditional heavy weight algorithms are not apt for IoT due to their constrained environment. Hence, alternate lightweight cryptography solutions symmetric as well as asymmetric can be used.

12. References

1. European Comission. Internet of Things in a Roadmap for the Future. 2008. p. 1-32.
2. Bojanova I, Hurlburt G, Voas J. Imagineering an Internet of Anything. Computer (Long Beach Calif). 2014; 47(6):72–7.
3. Kim I, Back M, Yim H, Lee K. RFID adaptor for detecting and handling data events in Internet of Things. Indian Journal of Science and Technology. 2015; 8(5):140-8.
4. Parks R, Pennsylvania T. RFID privacy issues in healthcare: Exploring the Roles of Technologies and Regulations. 2010; 6(3):1–24.
5. Xu B, Liu Y, He X, Tao Y. On the architecture and address mapping mechanism of IoT. IEEE International Conference on Intelligent Systems Knowledge Engineering; 2010. p. 678–82.
6. Mattern F, Floerkemeier C. From the internet of computers to the internet of things. Lecture Notes on Computer Science (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics). Vol. 6462. 2010. p. 242–59.
7. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. Comput Networks. 2002; 38(4):393–422.
8. Alcaraz C, Najera P, Lopez J, Roman R. Wireless sensor networks and the Internet of Things: Do we need a complete integration? 1st International Workshop on the Security of the Internet of Things; 2010. p. 1–8.
9. Khan R, Khan SU, Zaheer R, Khan S. Future internet: The Internet of Things architecture, possible applications and key challenges. 10th International Conference on Frontiers of Information Technology; 2012. p. 257–60.
10. Wu M, Lu T, Ling F, Sun J, Du H. Research on the architecture of Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering; 2010. p. 484–7.
11. Weber RH. Internet of Things – New security and privacy challenges. Comput Law Secur Rev. 2010; 26(1):23–30.
12. Sicari S, Cappiello C, Pellegrini F, Miorandi D, Coen-Porisini A. A security-and quality-aware system architecture for Internet of Things. Information Systems Frontiers. 2014. p. 1–13
13. Devadiga K. IEEE 802.15.4 and the Internet of Things. 2003. p. 4–7.
14. Feldhofer M, Dominikus S, Wolkerstorfer J. Strong authentication for RFID systems using the AES algorithm. Cryptographic Hardware and Embedded Systems – CHES. Vol. 3156. 2004. p. 357–70.
15. Derbez P, Fouque PA. Exhausting demirci-seluk meet-in-the-middle attacks against reduced-round AES. International Workshop on Fast Software Encryption; 2014. p. 541–60.
16. Hong D, Sung J, Hong S, Lim J, Lee S, Koo B, Lee C, Chang D, Lee J, Jeong K, Kim H, Kim J, Chee S. HIGHT: A new block cipher suitable for low-resource device.

Cryptographic Hardware and Embedded Systems – CHES. Vol. 4249. Springer; 2006. p. 46–59.
17. Lee J, Lim D. Parallel architecture for high-speed block cipher, HIGHT. International Journal of Security and its Applications. 2014; 8(2):59–66.
18. Wheeler DJ, Needham RM. TEA, a tiny encryption algorithm. Fast Softw Encryption. 1995; 1008(3):363–6.
19. Virmani D, Beniwal N, Mandal G, Talwar S. Enhanced Tiny Encryption Algorithm with Embedding (ETEA). International Journal of Computers and Technology. 2013; 7(1):1-9.
20. Bogdanov A, Knudsen L.R, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. Present: An Ultra-Lightweight Block Cipher. Berlin Heidelb: Springer; 2007. p.0 450–66.
21. International Standard ISO/IEC Information Technology - Security Techniques. Lightweight Cryptography. 2012.
22. Nyberg K. Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. 2015. p. 165-85.
23. Gawali DH. Rc5 Algorithm: Potential cipher solution for security in Wireless Body Sensor Networks (WBSN). Int J Adv Smart Sens Netw Syst. 2012; 2(3):1–7.
24. Biryukov A, Kushilevitz E. Improved cryptanalysis of RC5. Advances in Cryptology—EUROCRYPT'98. Vol. 1403. 1998. p. 85–99.
25. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978; 21(2):120–6.
26. Zhou X, Tang X. Research and implementation of RSA algorithm for encryption and decryption. Proceedings of 6th International Forum *Strategic Technology* (IFOST); 2011. p. 1118–21.
27. Jamgekar RS, Joshi GS. File encryption and decryption using secure RSA. Int J Emerg Sci Eng. 2013; 1(4):11–4.
28. Koblitz N. Elliptic curve cryptosystems. Math Comput. 1987; 48(177):203.
29. Eisenbarth T, Kumar S, Paar C, Poschmann A, Uhsadel L. A Survey of lightweight-cryptography implementations. IEEE Des Test Comput. 2007; 24(6):522–33.
30. Ayuso J, Marin L, Jara A, Skarmeta A. Optimization of public key cryptography (RSA and ECC) for 16-bits devices based on 6LoWPAN. 1st International Workshop on Security Internet Things. Tokyo, Japan; 2010. p. 1–8.