International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Study on Internet of Things Security and Lightweight Cryptography

Sarangi Oza*1, Dipti Mathpal2
*1Information Technology, Gujarat Technological University, Anand, Gujarat, India
2Computer Engineering Department, Gujarat Technological University, Anand, Gujarat, India

ABSTRACT

The Internet of Things (IoT) is the most hyped technology, which means that it is the hottest topic that has gained the most attraction of the researchers currently. In recent years, there have been huge amount of research have been done in different aspects of IoT. Internet of Things (IoT) connect to the Internet billions of heterogeneous smart devices with the ability of interacting with the environment. Meanwhile, providing privacy and security is an inseparable part of this technology. Without providing enough security, the promising benefits of this successful technology will be misused. In order to enjoy this new environment, security of constrained end nodes is important. If one of the nodes compromised, the network suffers seriously. However, it is not easy to implement sufficient cryptographic functions on constrained devices due to the limitation of their resources. This paper gives an overview of the lightweight cryptography, which can be implemented efficiently in constrained devices. This technology enables secure and efficient communication between networked smart objects.

Keywords: IoT, Security, Security Issue, Lightweight Cryptography, Cryptographic Algorithm

I. INTRODUCTION

The Internet of Things (IoT), sometimes referred to as the Internet of Objects, will change everything including ourselves. The Internet has an impact on education, communication, business, science, government, and humanity. Clearly, the Internet is one of the most important and powerful creations in all of human history and now with the concept of the internet of things, internet becomes more favorable to have a smart life in every aspect [1]. Internet of Things (IoT) is becoming a part of our daily lives, which will ease our daily life. With the rapid development of Internet technology and communications technology, our lives gradually led into an imaginary space of virtual world. People can chat, work, shopping, keeps pets and plants in the virtual world provided by the network. Whole generation is heading towards the world, which undoubtedly called a smart world. Trillions of objects will be connected over the internet, so that they can communicate with each other taking important decisions [3]. Managing such a huge amount of connections is a big challenge for network administrators. [2]

The connectivity is improved from any-time, any-place for any-one into any-time, any-place for any-thing. In the economy developments of IoT technologies together with ICT innovations helps to develop the infrastructures of their promotion and future strategies. The main aim is to allow interaction and integration of the physical world and the cyber space.

At present, more than 20 billion IoT gadgets are sent on the Internet, and this number is relied upon to increment in scale throughout the following five to 10 years. Kevin Ashton has used the term Internet of Things (IoT) for the first time, which is now gaining popularity. Current IoT gadgets generate immense measure of information named as large data, consequently we require a devoted computing framework to process this in close ongoing. An extensive variety of IoT applications incorporate transportation frameworks, Smart homes, Shrewd Industries, Media, and Medical and so forth. The IoT organize helps in the data handling and control of these applications. Internet of Things is fundamentally physically associated objects. Every physical object associated with each different structures in an IoT makes IoT network. The associated physical gadgets moreover implanted with various software, sensors and have network connectivity, which makes them able to share and access the information. [6]

The IoT is the whole thing other than a complete project. In fact, its realization faces several issues. Sociological challenges to faces issues differ as making people conscious and knowledgeable of technological challenges in the system design, data usability, security, and privacy for technology development as the main concept.

As to the security, the IoT will face issues that are more challenging. There are the following reasons: 1) the IoT extends the internet through the traditional internet, mobile network and sensor network and so on, 2) everything will be connected to this internet and 3) These things will communicate with each other. As a result, the new security and privacy problems will occur. We should give more awareness to the research issues for confidentiality, authenticity, and integrity of data in the IoT. [8]

II. IoT AND SECURITY

Security in IoT is a need to provide integrity, confidentiality, non-repudiation and authentication of the information flows. Moreover, mechanisms are needed to implement protection against threats to the normal functioning of IoT communication protocols.

A. Security Parameters

Based on the IoT security issues, the need of security is required for IoT system.

The parameters of security demand needs a safe internet system of things. They are as follows, [9]

IoT network security: Protecting and securing the network connecting IoT devices to back-end systems on the internet. IoT network security is a bit more challenging than traditional network security because there is a wider range of communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity. Key capabilities include traditional endpoint security features such as antivirus and antimalware as well as other features such as firewalls and intrusion prevention and detection systems.

IoT authentication: Providing the ability for users to authenticate an IoT device, including managing multiple users of a single device (such as a connected car), ranging from simple static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics. Unlike most enterprise networks where the authentication processes involve a human being entering a credential, many IoT authentication scenarios (such as embedded sensors) are machine-to-machine based without any human intervention.

IoT encryption: The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols. Moreover, all IoT encryption must be accompanied by equivalent full encryption key life cycle management processes, since poor key management will reduce overall security.

IoT PKI (Public Key Infrastructure): As an infrastructure, PKI is not one single 'thing'. Rather, it is a set of rules, policies and procedures – all based around the principal of digital certificates. These policies verify the ownership of public keys – that is, the disseminated keys that form one-half of public key cryptography pairs. Those pairs of keys achieve two crucial security functions: they **authenticate** the sender of information, and they **encrypt** that information – only the holder of the paired private key can decrypt the message on the public key. The key pairs are authenticated and bound to respective identities by digital certificates. In short, PKI provides a framework to both verify the identity of devices, and to protect the data transmitted between those devices. [13]

IoT security analytics: Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting on specific activities or when activities fall outside established policies. These solutions are starting to add sophisticated machine learning, artificial intelligence, and big data techniques to provide more predictive modeling and anomaly detection (and reduce the number of false positives), but these capabilities are still emerging. IoT security analytics will increasingly be required to detect IoT specific attacks and intrusions that are not identified by traditional network security solutions such as firewalls.

IoT API security: Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST-based APIs. API security will be essential for protecting the integrity of data transiting between edge devices and back-end systems to ensure that only authorized devices, developers, and apps are communicating with APIs as well as detecting potential threats and attacks against specific APIs.

III. IoT SECURE ARCHITECTURE

Real time working of IOT is possible through the integration of various technologies together. Security system such as trusted perception module, trusted terminal module and trusted network module. In this paper, a layered architecture of IOT is presented that gives an idea about basic architecture of IOT. Generally, IOT is divided into three layers: Perception layer, Network layer, and Application layer. Generally, the IoT can be separated into four key levels. Below Figure shows the IoT level architecture. [10]

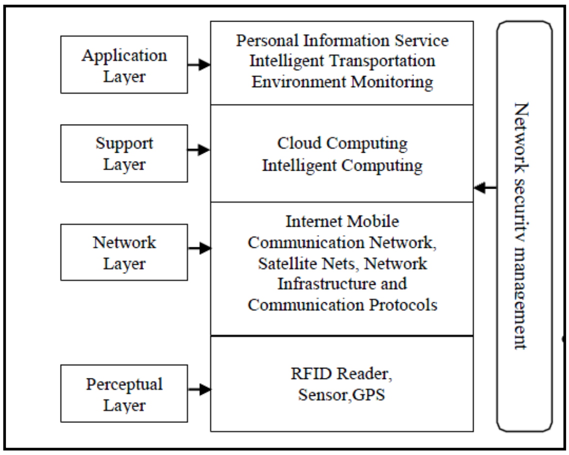
Application Layer
Personal Information Service
Intelligent Transportation
Environment Monitoring
Support Layer
Cloud Computing
Intelligent Computing
Network Layer
Internet Mobile Communication Network, Satellite Nets, Network Infrastructure and Communication Protocols
Perceptual Layer
RFID Reader, Sensor,GPS
Network security management

Figure 1. IoT Security Architecture [8]

Application Layer: Application layer is the most important in terms of users as it acts as an interface that provides necessary modules to control, and monitor various aspects of the IoT system. Applications allow users to visualize, and analyze the system status at present stage of action, sometimes prediction of futuristic prospects.

Support Layer: In the layer, data processing and intelligent decision of network behavior can be done. Intelligent processing is limited for malicious information, so it is a challenge to enhance the ability to recognize the malicious information.

Support layer requires a lot of the application security architecture such as cloud computing and secure multiparty computation, use strong encryption algorithm and encryption protocol, stronger system security technology and anti-virus.

- **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.

- **Perceptual Layer:** Generally perceptual nodes are less computer power and storage capacity because they are simple and with less power. Therefore, it is unable to use frequency hopping communication and public key encryption algorithm to security protection. In addition, it is very complicated to set up security protection system. Meanwhile attacks from the external network such as deny of service also carry new security issues. In the other hand of sensor data, still necessary to protect secure communication for integrity, authenticity and confidentiality. At initial node authentication is necessary to prevent protection from illegal node access, and before the data encryption key agreement is an important process in advance technology. Resources consumption is stronger and more secure for the safety measures to solve this issues, lightweight encryption technology becomes very important, which includes Lightweight cryptographic algorithm and lightweight cryptographic protocol.

IV. LIGHT WEIGHT CRYPTOGRAPHY

Cryptographic technologies are advancing: new techniques on attack, design and implementation are extensively studied. One of the state-of-the-art techniques is “Lightweight Cryptography (LWC)”. Lightweight cryptography is a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, health-care devices and so on. Lightweight cryptography also delivers adequate security. Lightweight cryptography does not always exploit the security-efficiency trade-offs. We report recent technologies of lightweight cryptographic primitives. We propose to adopt new advancing technology, “Lightweight Cryptography”, in the IoT. We describe two reasons that support our proposal.

1. Efficiency of end-to-end communication

In order to achieve end-to-end security, end nodes have an implementation of a symmetric key algorithm. For the low resource-devices, e.g. battery-powered devices, the cryptographic operation with a limited amount of energy consumption is important. Application of the lightweight symmetric key algorithm allows lower energy consumption for end devices.

2. Applicability to lower resource devices

The footprint of the lightweight cryptographic primitives is smaller than the conventional cryptographic ones. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices.

A. Lightweight Cryptographic Primitives[12]

In this, we discuss the different primitives of lightweight cryptographic algorithms as shown in Fig. 1 and we summarize many lightweight algorithms in the Table 1 based on their key size, block length, number of rounds and structures.

1) Lightweight Block Ciphers:

Xinxin Fan et al.'s research (Fan et al. 2013) presented a lightweight cipher WG-8 as a cryptographic algorithm, which is tailored from the Welch-gong cipher family for low-resource devices. A number of block ciphers have been proposed in existing research to achieve better performance for items such as AES-128 (Iokibe et al. 2014), RC-5 (Rivest 1994), TEA Wheeler and Needham (1994) and XTEA (Yu et al. 2011). Generally, some of these were improved and designed by simplifying conventional block ciphers to improve their performance. For an instance, DESL (Leander et al. 2007), which is also known as DES light weighted, which is a variant of classical DES (Saputra et al. 2003).

In DESL, the round function uses a single S-box rather than repeat eight rounds, which results in the creation of initial and final permutation to increase hardware implementation. SIMON and SPECK (Beaulieu et al. 2015), which are from block ciphers, come in a variety of width and key sizes. Both are flexible with given platforms and perform well across the full spectrum of lightweight applications. Block size should be smaller to get benefits of performance. It should be less than AES at 64-bits instead of 128-bits. When the block size decreases, it limits the size of plain text. Smaller key size In order to achieve power consumption with limited battery life, the key size must be small in a lightweight block cipher. For example, PRESENT (Bogdanov et al. 2007) is 80-bits in key size, and Twine (Hosseinzadeh and Hosseinzadeh 2016) is 80/128-bits in key size.

Simpler rounds Lightweight block ciphers that target low-resource constrained devices naturally have simple computation operations as compared with conventional block cipher algorithms. The number of rounds should be limited in lightweight design algorithms. For example, for a single S-box 4-bit S-boxes have been used in lightweight instead of 8-bit boxes in conventional cryptography. Some simpler lightweight cryptography algorithms are as follows: PRESENT uses 4-bit S-boxes, and Hummingbird2 (Mohd et al. 2015a) and Iceberg (Standaert et al. 2004) have only four rounds. Simpler key schedules for a given key, a key schedule is a kind of algorithm that calculates the sub keys for rounds. Complex keys consume more memory and energy for their implementations. As such, a lightweight block cipher utilizes simpler key schedules, which can generate sub keys. For example, the block cipher of TEA simply splits a 128-bit key into four 32-bit keys.

2) Lightweight Hash Functions

In 2006, Feldhofer and Rechberger brought up the absence of using lightweight hash function in RFID protocols (Feldhofer and Rechberger 2006). A conventional hash function has a large internal state size and high power consumption, which may not be preferred for resource-constrained devices. Some lightweight hash functions are PHOTON (Guo et al. 2011), Quark (Aumasson et al. 2013), SPONGENT (Bogdanov et al. 2011), and Lesamnta-LW (Hirose et al. 2010). For applications where collision resistance is not required, interior and balance sizes may be utilized. This can reduce the range of internal state.

3) Lightweight Stream Ciphers[14]

Stream ciphers are an alternative type of symmetric cryptosystem to block ciphers. They are based on the idea of the one-time pad (OTP) cipher, known as Vernam cipher [22]. OTP utilizes a completely random key stream, and each digit of the key stream is combined with one digit from plaintext to produce a digit of cipher text. OTP was proved to be unbreakable [23]; however, the key stream digits have to be completely random, and the key stream must have the same length as the plaintext.

Stream ciphers address these issues by sacrificing a degree of security: they apply a secret key, which is used to generate a pseudorandom key stream. The secret key is the symmetric key, and the pseudorandom key stream generated is used in the same way as the key stream in OTPs. However, the fact that the key stream is not completely random introduces security concerns. The key stream must be random enough to ensure that if an attacker knows the key stream, he cannot recover the secret key or derive the cipher's internal state.

Table 1. Summary of lightweight cryptographic algorithm

Algorith m	**Key Size**	**Block size**	**Structure**	**No of rounds**
AES	128/192/256	128	SPN	10/12/14
HEIGHT	128	64	GFS	32
PRESENT	80/128	64	SPN	31
RC5	0-2040	32/64/128	FEISTEL	1-255
TEA	128	64	FEISTEL	64
XTEA	128	64	FEISTEL	64
LEA	128,192,256	128	FEISTEL	24/28/32
DES	54	64	FEISTEL	16
SEED	128	128	FEISTEL	16
TWINE	80/128	64	FEISTEL	32
DESL	54	64	FEISTEL	16
3DES	56/112/168	64	FEISTEL	48
HUMMING BIRD	256	16	SPN	4
ICEBERG	128	64	SPN	16
PRIDE	128	64	SPN	20

B. Symmetric Lightweight Algorithm for IoT

Advanced encryption standard (AES), According to NIST, AES has three versions of Rijndael cipher, which are AES-128, AES-192 and AES-256. The encryption operation consists of 4 × 4 matrix that has 128 bit sized blocks. The internal state is organized by subbyte, shiftrows, mixcoloumn, and addroundkey. TWINE This utilizes Feistel structure which called 8 times per round and XOR operation on sub key and apply 4 × 4 S-box. Unlike CLEFIA and HIGHT, TWINE is more complicated permutation and combination to speed up diffusion. In TWINE, permutation only requires only half as many as rounds as the circular shift for single sub block difference to diffuse all sub-blocks. High security and lightweight (HIGHT) Height utilizes very simple and basic operation to work for Feistel network. That key is generated during the encryption and decryption phases.

Lee et al. proposed a parallel implementation which necessitate less energy, limited number of line of code, and improve the RFID system (Lee and Lim 2014). HIGHT has saturation attack vulnerability. PRESENT, This depends on SP-network and consists of 31 rounds. PRESENT is utilized as lightweight algorithm for security. It has a block length of 64 bits and two keys of 80 and 128 bits. For hardware implementation, it applied on substitution layer that utilizes 4-bits of input and the S-box output.

C. Asymmetric Lightweight Algorithms for IoT

RSA Generally, RSA does not belong to the lightweight cryptography system because of its large key size. Due to using two large prime numbers and performing modulo operation, RSA provides more security and maintains the privacy of users. Elliptic curve cryptography (ECC) Compared to the RSA algorithm, ECC requires a smaller key size. As such, it has a fast processing speed and requires less memory. Thus, it is applied to the small area of hardware implementation, which leads to faster computation in real time (Eisenbarth and Kumar 2007). The nodes in 6LoWPAN utilize the ECC algorithm, which can be applied to constrained devices.

V. 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. However, 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.

VI. REFERENCES

[1]. Zeinab Kamal Aldein Mohammeda ,Elmustafa Sayed Ali Ahmed,"Internet of Things Applications,Challenges and Related Future Technologies",World Scientific News 67(2) (2017) 126-148

[2]. Janani R,Siddique Ibrahim S. P,Kirubakaran R,"A Survey on Improving Security in Internet of Things (IoT) with SDN",International Journal of Scientific Research in Computer Science,Engineering and Information Technology (IJSRCSEIT),ISSN : 2456-3307,Volume 2,Issue 2,pp.1054-1058,March-April.2017

[3]. Priya Sharma,Tanya Sharma and Uma Rathore Bhatt. Article: Impacts of IoT: An Overview. IJCA Proceedings on National Conference on Contemporary Computing NCCC 2016(2):1-3,April 2017.

[4]. R. Hall,A. Rinaldo,and L. Wasserman,"Differential Privacy for Functions and Functional Data," Journal of Machine Learning Research,2013,pp.703-727.

[5]. J. Sathish Kumar,Dhiren R. Patel,"A Survey on Internet of Things: Security and Privacy Issues",International Journal of Computer Applications (0975-8887) Volume 90-No 11,March 2011

[6]. Navjot Jyoti "Internet of Things (IoT) : Security,Applications,Challenges and Future Directions",International Journal of Scientific Research in Computer Science,Engineering and Information Technology 2017 IJSRCSEIT,Volume 2,Issue 4,ISSN : 2456-3307

[7]. Chakib BEKARA,"Security Issues and Challenges for the IoT-based Smart Grid",Procedia Computer Science 34 (2014) 532-537,ELSEVIER

[8]. G. Ambika,Dr. P. Srivaramangai," A Study on Security in the Internet of Things", International Journal of Scientific Research in Computer Science,Engineering and Information Technology 2017 IJSRCSEIT ,Volume 2, Issue 6,ISSN : 2456-3307

[9]. https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-thinchnologiegs-iot-security-tes

[10]. Mayuri A. Bhabad,Sudhir T. Bagade,"Internet of Things: Architecture,Security Issues and Countermeasures",International Journal of Computer Applications (0975-8887) Volume 125-No.14,September 2015

[11]. P.P.Ray "A survey on Internet of Things architectures "Journal of King Saud University-Computer and Information Sciences (2016)

[12]. Masanobu Katagi and Shiho Moriai ,"Lightweight Cryptography for the Internet of Things" Sony Corporation

[13]. Saurabh Singh,Pradip Sharma,"Advanced lightweight encryption algorithms for IoT devices: survey,challenges and Solutions",Journal of Ambient Intelligence and Humanized Computing • April 2017

[14]. http://info.deviceauthority.com/blog-da/pki-iot-security

[15]. http://onlinelibrary.wiley.com/doi/10.1002/sec.1399/full