International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Lightweight Cryptography Algorithms for Internet of Things

R.Vasuki

Assistant Professor, Department of Computer Science, Mannar Thirumalai Naicker College, Madurai, Tamilnadu, India

ABSTRACT: In recent days, IoT or Internet of Things makes the internet revolution with the help of 5G technology in the world. It connects the physical objects in daily routine life. It directly impacts our lives through the smart devices. It deals with confidential data to connect the devices or the process of interconnection. Beside the IoT, Security plays important role in network to prevent the unauthorized access, misuses of data, monitoring and data, modification etc. The collection of data from the various device leads to cyber attacks. More encryption techniques are introduced in the wireless environment. But it consumes high power, more computational complexity etc. Light weight cryptography is an encryption method that uses less memory, less computing resource and less power supply to provide protection that can work over resource-limited devices. In this paper describes the light weight algorithms used for secure data transmission in the wireless networks.

KEYWORDS: Introduction of IoT, Encryption, Cryptography, Lightweight cryptography, Algorithms.

I. INTRODUCTION

With the implementation of 5G, Internet of Things (IoT) has become a center of attraction for almost all industries due to its wide range of applications from various domains. The enormous growth of industrial control processes and the industrial IoT implies unprecedented vulnerability to digital danger in critical infrastructure through the interconnected systems.

Characteristics of Security:
Reliability – Data accuracy and consistency.
Availability - Many devices are interconnected, we need to assure the accessibility of the device to get the required data.
Robustness – Quality of data or condition of being strong and in good condition.
Confidentiality - Information can only be accessed by the right person.
Integrity - The identities of sender and receiver are confirmed.
Data authentication – It is the important process because Needs to identify the right person to connect the device. It is the process of confirming the origin and integrity of data.

II. CRYPTOGRAPHY AND ITS CATEGORIES

To achieve the data security we need the help of Encryption. Encryption is the method by which message is converted into secret code that hides the information's original meaning. Cryptography is the science and it transforming the original messages to make them secure.
In computing, original data is also known as plaintext, and encrypted data is called cipher text. The technique used to encode and decode the message is called encryption algorithms or ciphers. The Cryptographic algorithms divide into two types.

1. **Symmetric Key Cryptography**

It is an encryption system where the sender and receiver used the same key for encryption & decryption. Symmetric key is more efficient while we compare with Asymmetric when we need to encrypt the lengthy messages. Symmetric Key Systems are faster and simpler but there is a problem in that because sender and receiver exchange the key in a secure manner.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

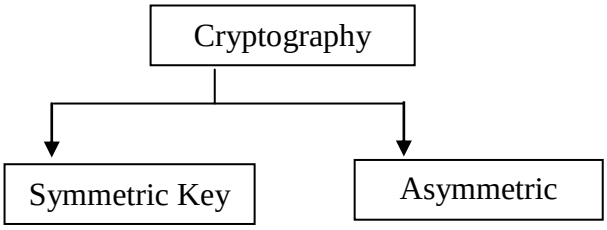

Fig 1: Types of Cryptography

I) Block Ciphers: It divides the data the plaintext into blocks and share the same key for encrypt and decrypt the block.

II) Stream algorithms. Encrypted data is kept in the Streams instead of systems memory. Some modern symmetric encryption algorithms are:

- Advanced Encryption Standard(AES) ,DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm),Blowfish (Drop-in replacement for DES or IDEA)
- CAST – 128 ,RC4 (Rivest Cipher 4),RC5 (Rivest Cipher 5),RC6 (Rivest Cipher 6)

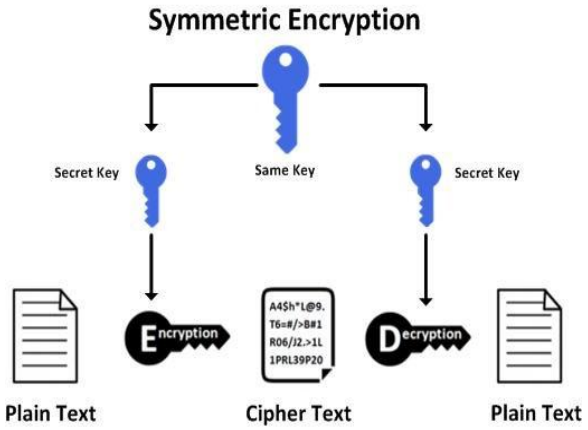

Fig 2: Symmetric Encryption

2. Asymmetric Key Cryptography:

In asymmetric key or public-key cryptography, there are two keys used for encrypt and decrypt information. There are Private Key and Public key .The private key kept by the receiver. The Public key delivered to the receiver. Public key and Private Key are not same. In case the public key is known to everyone they could not decode the message except the intended receiver. Because he alone knows the private key. Secured data transmission is the primary factor of asymmetric cryptography. It is highly secured encryption process because users are never required to reveal or share their private keys, thus decreasing the chances of a cybercriminal discovering a user's private key during transmission.

RSA: The RSA algorithm, named for its creators Ron Rivest, Shamir, and Adelman, is an asymmetric algorithm used all over the world, which is used to secure many common transactions such as Web and e-mail traffic [10].

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

It uses two numbers e and d for public and private keys. RSA derives its security from the computational difficulty of factoring large integers that are the product of two large prime numbers.

Diffie-Hellman key agreement:

Dr. Whitfield Diffie and Dr. Martin Hellman was developed Diffie-Hellman Key agreement in 1976 [10]. It was purely designed for key exchange. Diffie-Hellman Key agreement algorithm, both sender and receiver parties creates a symmetric session key to exchange the data without remember for future use. It is one time session key for two parties.

Elliptic Curve Cryptography:

ECC is considered as a powerful key approach for encryption and also it is an alternative for RSA.It produce security between key pairs for public key encryption by using the mathematics of elliptic curves equation.ECC key is significantly smaller than RSA. Size is essential advantage because it translates into more power into smaller devices. ECC generate keys that are more difficult
mathematically crack. It is more secure than RSA.

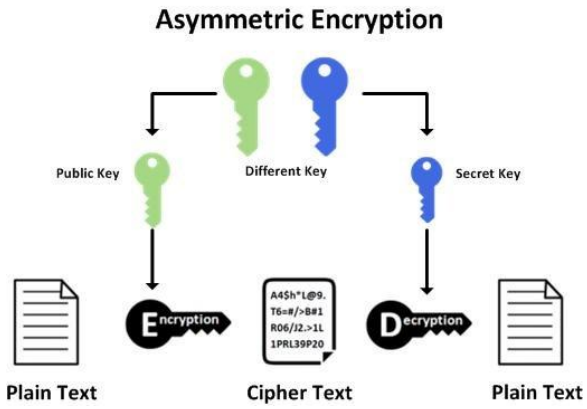

Fig 3: Asymmetric Encryption

In general conventional Cryptographic algorithm requires more computational power, memory capabilities. It does not scale well into a world with embedded systems and sensor networks. Thus, Light weight Cryptography methods are used to overcome the conventional cryptography for IoT.

Lightweight Cryptography

National Institute of Standards and Technology (NIST) put the effort to design a little-explored cryptographic concept. The concept names “Lightweight cryptography” and it purpose is “to design the cryptographic algorithm works with small and simple electronic devices without compromising the security. With the guidelines of NIST, millions of small and simple devices are include in the IoT to deal with current cryptographic mechanisms.

Light weight cryptography has been played a vital role for the fast few years. Lightweight cryptography is a cryptographic algorithm; it runs on small and resource constraints device. Light weight Crytography generally has

- Smaller memory Size
- Low Power Consumption
- Low Cost
- Smaller physical Size
- Optimized Speed

We need Cryptography algorithms with lightweight without compromising security.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Light Weight Cryptography design

Based on metrics discussed both in hardware and in software, most lightweight algorithms are designed to use lesser internal states, short block and key sizes. Indeed, most lightweight block ciphers use only 64-bit blocks (AES is demanded a 128-bit block and a 128-bit key). The lightweight execution usually leads smaller RAM consumption, and it is fine at processing smaller messages as well.

Light weight cryptography algorithms are reasonable for platforms like RFID (Radio Frequency Identification), FPGA (Field Programmable Gateway),etc.

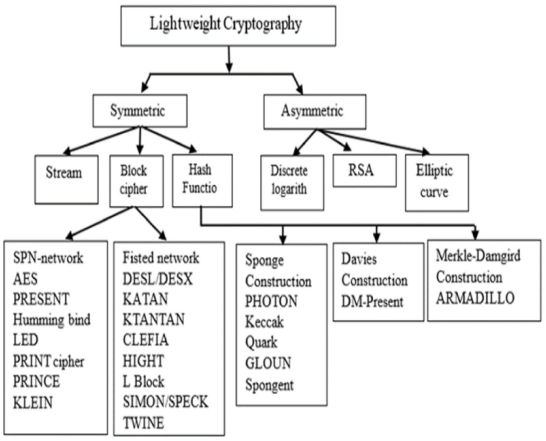

Fig 4: Lightweight Cryptography Algorithms

III. SYMMETRIC KEY CRYTOGRAPHY

- Block Cipher
- Stream Cipher
- Hash function

The most part of IoT calculation is done by these algorithms.

Stream ciphers:

1. 2005 Grain, Trivium
2. Mickey

Block ciphers:

1. 1977 DES,
2. 1989 GOST
3. 1997 XTE A
4. 1998 AES
5. 2005 mCrypton, STEA
6. 2006 Hight, SEA
7. 2007 Clefia, Kasumi DESL DESXL Present Kasumi, DESL, DESXL, Present
8. 2008 Puffin
9. 2009 Katan, Kantan32, Hummingbird, MIBS
10. 2010 PRINT
11. 2011 Klein, LED, Twine, EPCBC, Vitamin-B, Piccolo

Hash functions:

1. 2007 MAME
2. 2008 Squash DM

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

3. 2008 Squash, DM -Present H Present, H -Present Present, Keccak
4. 2010 Quark, Armadilo
5. 2011 Spongent, Vitamin-H, Photon

A. Block Cipher:

A block cipher mode of operation take a block of plaintext bits for encryption and produce a block of encrypted text bits with the same size.

Block cipher - a type of a symmetric cipher, which through continuous mapping (usually) processes information blocks (often 64 or 128 bits). "Lightweight" block cipher is different from the conventional block because it uses the algorithms that require less computing power. Popular lightweight cryptographic algorithms are

PRESENT: PRESENT is a block cipher regarded as being the predecessor of lightweight cryptography. It was published in 2007 and has been registered in ISO/IEC 29192. PRESENT is 64 bits and the key sizes are 80 or 128 bits [6]. It has a little circuit size that enables execution in the RFID tag, which is not possible using the standard AES encryption.

CLEFIA: CLEFIA - encryption algorithm, developed by Sony as a safe alternative to AES. It has 128,192 and 256 bit keys. The algorithm consists of two component parts: a key part of the schedule and data processing portion.

HIGHT: (high security and light weight) with 64-bit block length and 128-bit key length, which is suitable for low-cost, low-power, and ultra-light implementation. It has a 32-round iterative structure which is an alternate of generalized Feistel network.

GOST: Russian block encryption standard GOST 28147-89 [GOST 28147-89] has been known for more than twenty years and challenging algorithm an appropriate choice of replacement units. Simple design and low hardware requirements allowed using quite effectively on platforms with limited resources.

TEA (Tiny Encryption Algorithm) is a block cipher notable for its simplicity of description and implementation, typically a few lines of code. It was designed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory.

KATAN: The KATAN ciphers compose of three variants: KATAN32, KATAN48 and KATAN64. All the encryption in the KATAN family issues the key schedule which accepts an 80-bit key.

HUMMING BIRD: Hummingbird-2 is an well-known encryption mechanism that has been planned particularly for resource-constrained devices such as RFID tags, wireless sensors, smart meters and industrial controllers. It is the combination of block cipher and stream cipher. It developed with very small hardware or software footprint exclusively for constrained devices. It improves the speed of execution. It works with a 128-bit secret key and a 64-bit initialization vector.

PRINT: PRINT block cipher contains b-bit blocks (48, 96).There are specially designed for the purpose to explore the properties of IC- printing technology.

B. Stream Cipher:

Stream ciphers also widely used ubiquitous computing applications. Their speed and straightforwardness empower reduced and low-power usage, permit them to exceed expectations in applications relating to resource-constrained gadgets. The results of the International Organization for Standardization/International Electro technical Commission 29192-3 norm and the cryptographic rivalries eSTREAM and Competition for Authenticated Encryption. Security, Applicability, and Robustness are summed up beside the most recent outcomes in the field.

C. Hash Functions:

Many people attracted by the Hash function SHA-3 which was delivered by NIST's.SHA-3 is likely to be a common hash function, and any one of the existing finalists do not convince lightweight properties. Implementation of Hash functions in light weight cryptography is under in the research. They are too immature to adopt now. With the help of lightweight block ciphers able to built lightweight hash functions.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

2. PUBLIC KEY CRYPTOGRAPHY

While lightweight public key primitives are in demand for key management protocols in smart objects networks, the required resource for public key primitives is much larger than that of symmetric key primitives be implemented with fairly small footprint, but they cannot carry out within a reasonable time [7].

IV. CONCLUSION

Embedded devices penetrate our lives, carrying us closer to the vision of universal processing. This huge change in the structure, number and utilization of figuring gadgets, presents new difficulties as far as the security of their assets, just as the related information that are put away or sent. This paper introduced an overview of lightweight cryptographic algorithms for embedded devices. Normalized and novel stream figure plans were broke down, additionally including validated encryption plans. Lightweight cryptography having more capable to secure the smart devices because of its efficiency and smaller in size. We consider that lightweight primitives should be implemented in the networks. Lightweight block ciphers are more convenient to use in IoT.

REFERENCES

[1] https://www.futurex.com/blog/introducing-lightweight-cryptography
[2] https://www.tandfonline.com/doi/full/10.1080/23742917.2017.1384917
[3] https://eprint.iacr.org/2015/303.pdf
[4] https://www.researchgate.net/publication/316078586_A_review_of_lightweight_block_ciphers
[5] http://www.networksorcery.com/enp/data/encryption.htm
[6] https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html
[7] https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf
[8] https://link.springer.com/article/10.1007/s11277-020-07134-3
[9] https://arxiv.org/pdf/1704.08688.pdf
[10] Data communication and Networking by Behrouz A Forouzan
[11] https://internetofbusiness.com/nist-demands-lightweight-cryptography-to-protect-iot-devices/