International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Lightweight Cryptography to Secure Internet of Things(IoT)

Vrushali Ramesh Kadam[1], Priyanka Srinivas Naidu[2]

[1]*Vrushali Ramesh Kadam, Department of Master of Computer Applications, ASM IMCOST, Mumbai, India*
[2]*Priyanka Srinivas Naidu, Department of Master of Computer Applications, ASM IMCOST, Mumbai, India*

Abstract - *In Internet of Things (IoT), the huge connectivity of devices and massive data on the air have made information liable to different type of attacks. Cryptographic algorithms are used to provide confidentiality and maintain the integrity of the data. Lightweight cryptography could be a developing term which secures the information in an improved way utilizing low assets and giving higher throughput, conservativeness and having low power utilization. Lightweight algorithms are for the foremost part utilized as part of IoT innovation more model security with least memory and power utilization. The primary goal of cryptography is to secure the information specified lone the sender and beneficiary can determine and work the information and no other pariah or intruder can perceive or operate it.*

Key Words: **Lightweight Security; Internet of Things (IoT); Lightweight cryptography; Lightweight block ciphers; Lightweight stream ciphers; Lightweight hash functions**

1. INTRODUCTION

Internet of Things (IoT) is an emerging concept, which envisages to connect billions of devices with one another. The IoT devices sense, collect, and transmit important data from their surroundings. This exchange of very great amount of information amongst billions of devices creates an enormous energy need. IoT could be a term that envisions the connectivity between a physical and a digital world by using latest and felicitous technologies. IoT has been one amongst the recent topics within the technology domain for the previous few years and it's expected to revolutionize the globe kind of like that the internet itself did.
Internet of things (IoT) consists of several interconnected devices which continuously share information and data among one another. To protect that information, we need to understand the basic characteristics of security for IoT devices:
• Confidentiality- We need to make sure that the knowledge is just available to the authorized users.
• Availability- Multiple devices are connected, we need to make sure a device or tools gets its required data when it needs.
• Integrity- We need to make sure that the data or information is accurate.
• Authentication- This is an important characteristic but difficult to implement from IoT perspective. Its different entities connected which have different purposes and levels within the whole structure.
• Heterogeneity- It's different entity of the network contains a different function, complexity, and even different manufacturer. So, therefore, we need to ensure the Heterogeneity of the network too.
• Key Encryption- This is the most important step that is to ensure a secured connection, the devices and therefore the other entities need to have a light-weight key management system.
Over time, security of knowledge and key transmission have led to the thought of cryptography. Cryptography may be a process of securing the information from unauthorized access by transforming the information into an unrecognizable and unrelatable form.

In this paper, we have surveyed recent research work about different aspects of security solution for IoT. We have covered comprehensively a flow of security measures from Lightweight Cryptographic solutions to comparison among different types of block ciphers. We have also included comparison between Hardware and Software solutions and different recent approaches of the foremost promising and researched block cipher, Advanced Encryption Standard (AES), for IoT security.

On a replacement computing environment called "Internet of Things (IoT)" or "Smart Object" networks, a plenty of constrained devices are connected to the Internet. The devices interact with one another through the network and supply new experience to us, so as to enjoy this new environment, security of constrained end nodes is very important. If one among the nodes were compromised, the network may be suffered seriously. However, it is difficult to implement sufficient cryptographic functions on constrained devices due to the limitation of their resources.

The IoT are unleashing the subsequent wave of innovations because of its inherent capability of connecting intelligent 'things' in an exceedingly physical world into cloud-based information technology architecture. In the IoT, many interconnected resource-constrained devices aren't designed to hold out expensive conventional cryptographic computation, which makes it difficult to implement sufficient cryptographic functions. To guarantee security and privacy protection within the IoT becomes a significant concern when integrating resource-constrained devices into the IoT securely since they're incapable of closing sufficient cryptographic algorithms.

The mechanism of IoT consists of several elements like Identification, sensing, communication, computation,

services and semantics. Identification is that the most significant one because it ensures that the specified data or service reaches to the proper address. Sensing deals with the gathering of the data from different resources and this information is then sent to data-centers. This data is then analyzed using different conditions and parameters for the aim of assorted services. The sensors may be wont to collect humidity, temperature etc. Communication in IoT performs the mix of heterogeneous objects to supply specific services. Communication is typically performed by using Wi-Fi, Bluetooth etc. Computation is performed by different microcontrollers, microprocessors, Field Programmable gate arrays and plenty of software applications. Services may be associated with identity, information aggregation, collaborative or ubiquitous. Lastly, Semantics deals with the intelligent knowledge gathering to create decisions.

During this paper, we discussed about Lightweight Cryptography, the two main division of Cryptography, referred as Asymmetric key Cryptography and Symmetric key Cryptography. We have also discussed and gathered different types of Stream Ciphers and Block Ciphers which are possibly suitable for IoT applications.

2. Challenges in lightweight cryptography

Lightweight cryptography targets a very wide variety of resource-constrained devices such as IoT end nodes and RFID tags that can be implemented on both hardware and software with different communication technologies. It is very difficult for resource-limited environment to implement the quality cryptographic algorithms thanks to the implementation size, speed or throughput and energy consumption. The lightweight cryptography trade-offs an implementation for cost, speed, security, performance and energy consumption on resource-limited devices. The motivation of lightweight cryptography is to use less memory, less computing resource and less power supply to provide security solution that can work over resource-limited devices. The lightweight cryptography is expected simpler and faster compared to conventional cryptography. The disadvantage of lightweight cryptography is less secured.

2.1 Hardware implementation:

If the primitive is implemented in hardware, the subsequent metrics describe the efficiency of the implementation.

• The memory consumption and therefore the implementation size are lumped together into its gate area which is measured in Gate Equivalents (GE). The lower it's, the better.
• The throughput, measured in bits or bytes per second, corresponds to the quantity of plain text processed per unit of time. The upper it's, the better.
• The latency, measured in seconds, correspond to the time taken to get the output of the circuit once its input has been set. The lower it's, the better.
• The facility consumption, measured in Watts, quantifies the quantity of power needed to use the circuit. The lower it's, the better.

In hardware implementation of the lightweight cryptography, the code size, the memory consumption (RAM) and energy consumption are an important metrics. To well evaluate the lightweight cryptography, the precise sort of circuit (such because the clock), memory, storing of the interior states and key states should be taken into consideration. However, it doesn't mean that shorter block and key size are better since it should cause insecure against related-key attacks. In some case, the read-only 'Mask' technology is employed to burn keys into devices (chips) to scale back the key space. In recent, in, an energy efficiency of hardware implementation metric is proposed, within which the latency is employed to gather the time taken to perform a given operation.

2.2 Software implementation:

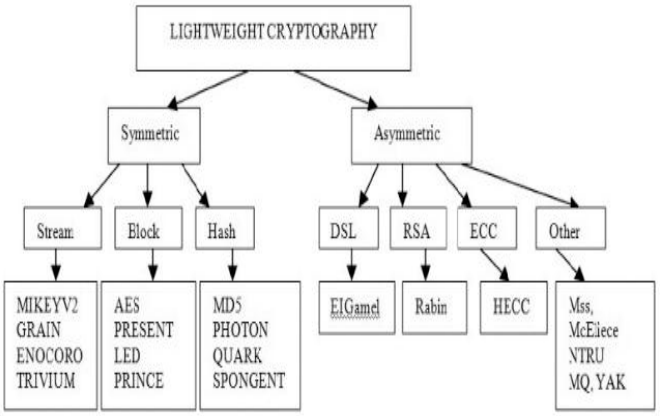
Lightweight primitives can be also implemented in software, typically for use on microcontrollers. In this case, the relevant metrics are the RAM consumption, the code size and therefore the throughput:

• RAM consumption corresponds to the amount of data which is written to memory during each evaluation of the function,
• The code size is the fixed amount of data which is needed to evaluate the function independently from its input, and
• As before, the throughput measures the average quantity of data which is processed during each clock cycle.

The first two are measured in bytes and should be minimized while the latter is measured in bytes per cycle and should be maximized. Again, these three quantities are not independent. Therefore, limiting the number of such operations leads to a decrease in both RAM consumption and an increase in throughput. In software implementation case, the implementation size and RAM consumption and also the throughput (bytes per cycle) are preferable metrics for the lightweight applications. The smaller, the better.

3. Lightweight Cryptography Encryption

There are different types of cryptographic solutions that are available to safeguard our important data but unfortunately not all of them are suitable for resource constrained environments like IoT devices. Lightweight cryptographic solutions are being researched thoroughly with an aim to own area efficient and power efficient solution. Both commercial and industrial IoT devices are prone to IoT specific attacks. The current cryptographic primitives can be divided into two categories. Asymmetric key cryptography and Symmetric key cryptography.



3.1 Symmetric Encryption:

Symmetric encryption uses the same key for both encryption and decryption of data. This method of encryption is secure and relatively faster. The major drawback of symmetric key encryption is the sharing of the key between the two communicating parties. An attacker can decrypt the data if he has access to the key. Symmetric key algorithms assure the confidentiality and integrity of data but do not guarantee authentication. This type of encryption uses three types of algorithms based on hashing, stream and block ciphers.

3.1.1 Hashing: A stream cipher is a symmetric key cipher in which plaintext digits are combined with a pseudorandom cipher digit stream. In this type each plaintext digit is encrypted one at a time with the analogous digit of the key stream, to give a digit of the cipher text stream as a result. Mickey V2 is a lightweight stream cipher and was written by Steve Babbage and Matthew Dodd. It creates a key stream from an 80-bit key and a variable length initialization vector (of up to 80 bits). The keystream has a maximum length of 240 bits [9]. Trivium is also one lightweight stream cipher and it was developed by Christophe De Canniere and Bart Preneel and has a low footprint for hardware. It uses an 80-bit key and generates up to 264 bits of output, with an 80-bit IV [10]. Grain and Enocoro are the Light Weight Stream Ciphers which have 80 bit and 128-bit key respectively. Grain has relatively low power consumption and memory [11]. Ecarno is defined by Hitachi and is included in ISO/IEC 29192 International Standard for a lightweight stream cipher method.

3.1.2 Streaming: A stream cipher is a symmetric key cipher in which plaintext digits are combined with a pseudorandom cipher digit stream. In this type each plaintext digit is encrypted one at a time with the analogous digit of the key stream, to give a digit of the cipher text stream as a result. Mickey V2 is a lightweight stream cipher and was written by Steve Babbage and Matthew Dodd. It creates a key stream from an 80-bit key and a variable length initialization vector (of up to 80 bits). The keystream has a maximum length of 240 bits. Trivium is also one lightweight stream cipher and it was developed by Christophe De Canniere and Bart Preneel and has a low footprint for hardware. It uses 80-bit key and it generates up to 264 bits of output, with an 80-bit IV.Grain and Enocoro are the Light Weight Stream Ciphers which have 80 bit and 128-bit key respectively. Grain has relatively low power consumption and memory. Ecarno is defined by Hitachi and is included in ISO/IEC 29192 International Standard for a lightweight stream cipher method.

3.1.3 Block: A block cipher is an encryption method that applies a deterministic algorithm together with a symmetric key to encrypt a block of text, instead of encrypting one bit at a time as in stream ciphers. PRESENT and CLEFIA for block methods are defined as standards for lightweight cryptography within ISO/IEC 29192-2:2012. One among the primary to indicate promise for a replacement for AES for lightweight cryptography is PRESENT. It operates on 64-bit blocks and uses a substitution-permutation method. CLEFIA could be a well-known lightweight block cipher was defined by Sony and has 128, 192 and 256-bit keys and 128-bit block sizes. Many lightweight cryptography algorithms were developed among them several symmetric algorithms use AES (Advanced encryption standards) as a customary.

3.2 Asymmetric Encryption:

Asymmetric cryptography is a cryptographic system that utilizes two types of keys; public keys that may be distributed widely and private keys which are known only to the owner. The generation of the public keys depends on cryptographic algorithms based on one way mathematical functions. Thus the public key can be openly distributed without compromising security as for achieving effective of security the requirement is keeping the private key private. In such this type of systems, any person can encrypt a message using the receiver's public key, but the encrypted message can only be decrypted with the receiver's private key. Asymmetric ciphers are computationally far more demanding than their symmetric counterparts. There are conventional asymmetric algorithms such as Rabin/RSA which is based on integer factorization problem, ECC/HECC which are based on Elliptic Curve Discrete Logarithm Problem.

There are some application specific asymmetric algorithms which are known for their performance and their resistance to quantum computer based decryption approaches, such as MSS, NTRU, McEliece, MQ, YAK. Merkle Signature Scheme (MSS) is a hash based cryptography and uses typical AES based hash functions. It is popular because of its smaller code size and faster verification process them RSA and ECC. NTRU is one of the open source public key cryptosystems that utilizes lattice-based cryptography for encryption and decryption of data. NTRU was patented but was placed in the public domain in 2017. It has two algorithms NTRUEncrypt, for encryption, and NTRUSign, for digital signatures. Like other prominent public key cryptosystems, it is also resistant to attacks using Shor's algorithm and its

performance is significantly better. Regarding the performance of NTRU in equivalent cryptographic strength, it should be noted that NTRU executes costly private key operations much faster than RSA. Performance time of RSA private operation increases as the cube of the key size, while as that of an NTRU operation increases quadratically. NTRU provides the same level of security comparable to RSA and ECC and therefore is highly efficient and suitable for embedded system. RSA is 200 times slower in key generation and almost 3 times slower in encryption and about 30 times slower in decryption as compared with NTRU. The drawback of NTRU is that it produces larger output, which may lower the performance of the cryptosystem if the number of transmitted messages is complex and crucial but it is safe when it is implemented when the recommended parameters are used.

McEliece is an asymmetric algorithm which was not largely accepted because of its larger public and private key matrices as compared to RSA. The encryption and decryption are faster than RSA. McEliece was not used to produce signatures, but the signature has been constructed based on Niederreiter scheme which is a variant of McEliece. From a security point of view, Niederreiter provides the same security level as McEliece. MQ requires 9690 bytes for the public key and 879 bytes for the private key and is based on the problem of solving multivariable quadratic equations over finite fields. It is commonly accepted that multivariate cryptography is more successful for building signature schemes basically because multivariate schemes give the shortest signature among quantum resistant algorithms.

4. Literature Survey

On April 18th, 2018, the National Institute of Standards and Technology (NIST) to develop a little-explored cryptographic concept. The concept is named "lightweight cryptography", and its purpose in keeping with NIST is "to develop cryptographic algorithm standards which will work within the confines of an easy device." NIST made their announcement in response to the burgeoning development of the web of Things (IoT), a network of sensors, monitors, cameras, and devices working together to make smart infrastructure. Without the IoT, none of those systems could perform the various, simultaneous communications necessary for his or her existence.

According to NIST, the tiny and straightforward nature of the voluminous electronic devices making up the IoT makes them unequipped to process current cryptographic algorithms. Lightweight cryptography would demand far fewer resources from the devices and take less time to finish their essential processes. Using costly heavy-weight solutions for every small device within the IoT would also make the worth of devices impractical for the organizations implementing solutions.

Because simple-device solutions usually depend upon symmetric cryptography, a version of cryptography within which senders and recipients of messages have the identical digital key to encrypt and decrypt messages, NIST specifies that the lightweight cryptography algorithms must use "authenticated encryption with associated data," or AEAD. AEAD means that the recipient of a message can use authentication to verify the integrity of both the encrypted and unencrypted information within the message. This ensures that messages are coming from who they say they are, and that the content of the message has not been altered in transit.

The 2018 announcement came together with a call for participation for help from the cryptographic community. NIST released a call for participation form called Draft Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. the aim of this exercise, a "crypto algorithm bake-off" if you'll, is to hunt submissions from leading cryptographers and industry experts so as to visualise and plan the implementation of lightweight cryptography within the IoT. in step with the NIST website, their goal is to "produce the type of encryption algorithms that developers agree will help." The submission period is now closed, and therefore the candidate algorithms are available for review on the NIST website. The chosen top respondents to the draft are currently participating in workshops to further develop their plans for the new algorithms. These talks are scheduled to continue through the end of 2020, at which point more information will be released to the public.

Lightweight cryptography is approaching on the horizon of lightweight cryptographic solutions. Because the IoT expands and projects like self-driving vehicles or the smart city develop around it, lightweight cryptography will likely become an integral a part of daily urban life. to stay up to this point on this important initiative in IoT data security, make certain to test back with Futurex for the newest news and developments.

5. CONCLUSIONS

In this paper, we discussed comprehensively a flow of lightweight security solutions for Internet of Things (IOT). We surveyed research work on Asymmetric key cryptographic and Symmetric key cryptographic (Stream Ciphers and Block Ciphers) for IoT. Lightweight cryptography contributes to the protection of smart objects networks thanks to its efficiency and smaller footprint. Lightweight cryptography has received an increasing attentions from both academic and industry within the past years. Conclusively this paper wraps up with proficient data for Hardware/Software for a particular application. In the future, we shall still contribute to secure IoT systems via research into the cryptographic technologies as discussed during this paper.

REFERENCES

[1] Internet Security Threat Report. (2019). Vol. 24, Symantec

[2] Dhanda, S. S., Singh, B., & Jindal, P. (2019). Wireless technologies in IoT: Research challenges. In K. Ray, S. Sharan, S. Rawat, S. Jain, S. Srivastava, & A. Bandopadhyay (Eds.), Engineering vibration, communication and information processing. Lecture Notes in Electrical Engineering, Vol. 478. Springer, Singapore.

[3] Sattar B. Sadkhan, Akbal O. Salman. "A Survey on Lightweight-Cryptography" 2018 International Conference on Advances in Sustainable Engineering and Applications (ICASEA). pp. 105–108. 2018.

[4] Shamsher Ullah, Xiang-Yang Li, Lan Zhang. "A Review of Signcryption Schemes Based on HyperElliptic Curve" 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM). pp. 51–58. 2017.

[5] Biryukov, Alex and Leo Perrin. "State of the Art in Lightweight Symmetric Cryptography." IACR Cryptology ePrint Archive P. 511. 2017.

[6] Alex Biryukov, Gaetan Leurent, and Arnab Roy. "Cryptanalysis of the "kindle" cipher". In Knudsen and Wu [KW13], pp. 86–103, August 2012.

[7] W. Zhang et al., RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," in Science China Information Sciences, vol. 58(12), pp. 1–15. 2015.

[8] R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers, in Proceedings of the 52nd Annual Design Automation Conference, pp. 1–6. 2015.

[9] Thierry Pierre Berger, Julien Francq, Marine Minier, and Gaël Thomas. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. IEEE Transactions on Computers, pp. 99, August 2015.

[10] Nizamuddin, S. A. Chaudhry, W. Nasar, and Q. Javaid, "Efficient Signcryption Schemes based on Hyperelliptic Curve Cryptosystem," IEEE International Conference on Emerging Technologies (ICET 2011), pp. 84–87, September 2011.