A Review on Lightweight Cryptographic Solutions in Internet of Things

[1] Ms. Shilpa V. Shankhpal, [2] Dr. Brahmananda S H
[1]Research Scholar, [2]Professor
[1] Department of Computer Science and Engineering
[1]Gitam School of Technology, Bengaluru Campus, GITAM, Bengaluru, India

Abstract: ***Internet of Things (IoT) is a network of physical devices like vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and connectivity which allows these devices to connect and transfer data. This allows the efficient and smart solutions for communicating with the heterogeneous devices. Thus, IoT opens up the key issues such as bandwidth, security, power, privacy and scalability. Among these, the Security and Privacy are main concerns or vital elements that need to be addressed to perform secure data exchange among devices in IoT. The current solutions for security at each layer are still vulnerable for attacks. This paper encloses the comparative analysis of various lightweight cryptographic algorithms used as solutions for IoT security issues. The paper also provides the brief study of algorithms with various possible attacks and more security issues that can occur in IoT environment. At last, paper encloses various opportunities and challenges based on the IoT security lightweight cryptographic solutions.***

Index Terms - Internet of Things, Security, Privacy, Lightweight Cryptography

I. INTRODUCTION

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

The major concern of the Internet of Things is associated with trust, confidentiality and security as the data transfer will be significantly high in future, the stronger security models must be developed and provided for secure and efficient data transmission over the IoT [1]. There are several licensed and unlicensed bands available for communication. It is mentioned that in IoT, the devices can be connected through wireless connections like RFID, Bluetooth, ZigBee, WSN, WLAN or Wi-Fi.

As IoT devices tend to have limited resources, bandwidth, power and also storage capability, it gets very complex to implement cryptography on these individual devices. Due to need for minimal human intervention in IoT, it makes the system more vulnerable for attacks like DoS and Man-In-the-Middle attack. Also, there are high chances that device gets accessed by illegitimate user, that might harm the system and lead towards the disaster. Thus, making data more secure is one of the key challenges in IoT. For this, lightweight cryptographic solutions/algorithms can be implemented in a resource inhibited environment such as various sensors, multiple sensor nodes, smart cards and so on. ISO 29192 is the standardized lightweight cryptography project that discusses lightweight attributes based on the target platform.

There are two important attributes in lightweight cryptographic solutions. One considers the hardware part of implementation that are energy consumptions as well as the size of the hardware. The other focuses on software part of implementation such as RAM occupancy and code length. The recent lightweight cryptographic solutions are discussed in further sections.

With the increase in application requirements of a user, a vast amount of data will be shared in future in IoT. Thus, the various security services in lightweight cryptographic solutions need to be provide to ensure,

Confidentiality- Data at rest or in transit 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 in IoT.

This paper is standardized as follows: Section II emphasizes a literature survey on IoT security architecture, their relevant challenges and existing cryptographic symmetric and asymmetric lightweight cryptographic algorithms are compared. The section III includes related work on existing lightweight cryptographic schemes for IoT and also their security concerns are covered. Section IV includes the possible attacks that might occur on existing algorithms/schemes in terms of opportunities and challenges in those cryptographic algorithms.

II. LITERATURE SURVEY

The structure of IoT is basically divided into 3 layers. Each of these layers has their own role and characteristics. Thus, potential security issues have been divided based on these three layers. The layers are [2],

- **Physical Layer/Perception Layer**: It's the basic layer of IoT where the main function of this layer is to gather or perceive information. For example, temperature sensors, RFID readers, barcode scanners, etc.
- **Network Layer**: This layer combines the functions of network as well as transport layer. It transmits the data through internet and mobile telecommunication in the form of data packets. As, the physical layer acquires huge amount of data which is then transmitted to network layer, hence, it needs certain information processing and management ability.
- **Application Layer**: This layer processes data intellectually so that processed information can be available for personal use.

Corresponding to three layer IoT architecture, a new security model is being developed for providing security at these three layers called as Multi-layer security architecture shown in Fig. 1.

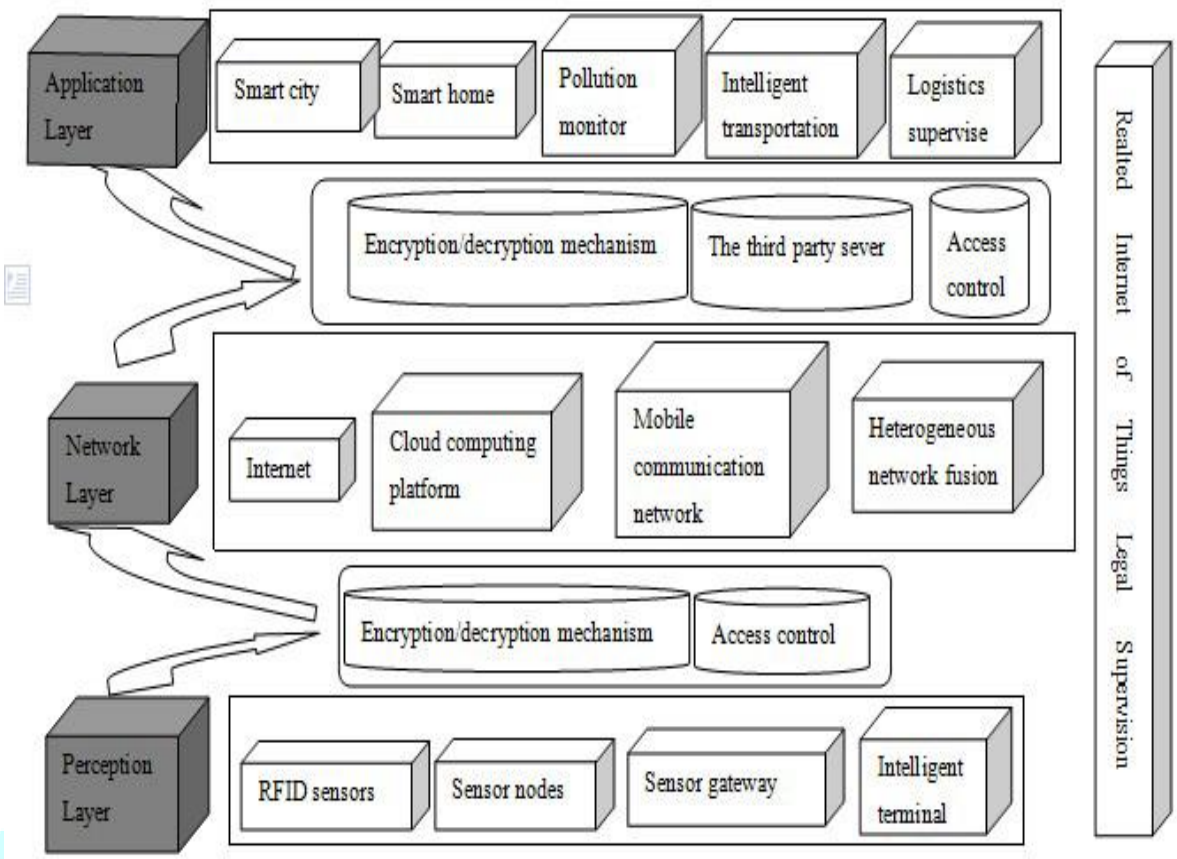

Fig. 1Multi-Layered IoT Security architecture

There are some existing security protocols present at each layer provided by multi-layer IoT security architecture. But, these protocols are not sufficient to provide data integrity and security at each layer. Thus, there are some attacks mentioned which can penetrate this multi-layered IoT security architecture. The table 1 shows list of security protocols in each layer along with the possible attacks that might occur.

TABLE I
SECURITY PROTOCOLS AND POSSIBLE ATTACK AT EACH LAYER

Layer	**Security Protocol**	**Possible Attacks**
Application	Not Fixed, designed by user	Depend on protocol
Network	DTLS, IPSec	Attack on RC4, Dos attack
Perception/Physical	IEEE 802.15.4 security	DoS, Authentication attack, Integrity attack

The CoAP (Constrained Application Protocol) was using IPSec and DTLS for securing data transmission in IoT. But, the predefined security protocols are vulnerable to aforementioned attacks. Thus, there are various cryptographic algorithms which can be symmetric or asymmetric. The symmetric algorithms use a one non public key for communication and sender and receiver use the same key for communication [15]. It ensures privacy and integrity of data; however it does not provide authenticity of data. There are various symmetric algorithms like AES, DES, Triple DES, Blowfish, IDEA that are compared on their properties like their data size, key size, number of rounds and existing threats shown in Table 2.

Meanwhile, Asymmetric algorithms use pair of public and private key for communication. Asymmetric ensures confidentiality, authentication and integrity. The most common algorithms are RSA by Rivest, Diffie-Hellman Key Exchange Algorithm, Elliptic Curve Cryptography (ECC) and Hash Functions.

The traditional symmetric and asymmetric algorithms are not used IoT environment as the IoT devices have low computation power, limited memory and limited power consumption. Thus, lightweight security algorithms were proposed for IoT. These algorithms are having small key size, memory requirements and execution time.

A. Symmetric Cryptographic Algorithms

Advanced Encryption Standard (AES) - It is specifically applied in CoAP at application layer. It is a symmetric block cipher that works on substitution permutation network with 4*4 matrix whose block length is 128-bits. The key size varies from 128, 192, 256-bits. This algorithm is sensitive for man-in-the-middle attack.

High Security and Lightweight (HIGHT) -This encompasses operations such as addition mod 2^8or XOR operation. The block size is of 64 bits and it works in 32 rounds on 128 bit keys. This algorithm cannot withstand saturation attack.

Tiny Encryption Algorithm (TEA) -This algorithm is applied in a limited environment such as sensor networks. It is a small block of code that only performs elementary operations such as XOR, ADD and SHIFT. It uses block size of 64 bits and 128 bit keys. Due to its simple XOR, adding and shifting operation, this is still vulnerable for many attacks.

PRESENT -This works on the basis of 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 comprises of 80 or 128-bits key and works on 64-bit blocks. It is still vulnerable to differential attack.

RC5 - This is specifically applied in Wireless Sensor networks. The RC5 designed as w/r/b, where w signifies word size, r represents number of working rounds, and b stands for number of bytes in encryption key. It is basically applied on 32-bit size but it also works on 16, 32, and 64. It is also vulnerable to differential attack.

TABLE III

A COMPARATIVE ANALYSIS OF SYMMETRIC LIGHTWEIGHT CRYPTOGRAPHY ALGORITHM IN IoT

Symmetric Algorithms	Code Lengths	Number of Rounds	Key Size	Block Size	Possible Attacks
AES	2606	10	128	128	Man-in-the-Middle attack
HIGHT	5672	32	128	64	Saturation Attack
TEA	1140	32	128	64	Related Key Attack
PRESENT	936	32	80	64	Differential Attack
RC5	Not Fixed	20	16	32	

B. Asymmetric Cryptographic Algorithms

RSA - This works by selecting two large prime numbers and generating public-private key pair. Find their modulus and selecting at random their encryption key and finally calculating the decryption key. In this, public key in propagated openly whereas private key is kept secret.

Elliptic Curve Cryptography (ECC) - Its key requirement is less as compared to RSA. Hence, it executes fast and consumes less storage. It is built on algebraic system where it takes two points on elliptic curve. The key is generated using discrete logarithm problem. ECC is more augmented for 6LoWPAN nodes by using bit shifting operation instead of multiplication to use for low powered devices.

III. RELATED WORKS

There are number of lightweight cryptography algorithms/schemes are present that minimizes the vulnerability of number of possible attacks in IoT. In [3], a new algorithm based on existing IBE (Identity Based Encryption) is introduced named as Fuzzy IBE. It allows private key for an identity, ω, to decrypt the cipher text encrypted with an identity ω', if and only if these identities are close to each other which is measured by 'set overlap' method. The error tolerance between the public and private key is used for the encryption process.

New ABE scheme having non-monotonic access structures is expressed in [4]. It allows user's private key to be expressed in any accessing formula. The proof of security is based on assumptions of bilinear Diffie-Hellman. This is less resource consuming as it includes key policy with non-monotonic structure.

In [4], the decryption of data is possible only if attributes satisfy the encrypted data access structure. This method is effective to integrate both data access and cipher text policies. In [5], a new public key is described and support for complex access policies with NOT, AND and OR gates and it is provided by attribute based broadcast encryption scheme. The security is proven by generic group with pairing and the comparison is done for network bandwidth requirements and information costs.

The [6] proposes the fast decryption scheme that uses the same constant number of pairs for decryption of cipher texts. The proposed scheme can be used to decrypt GPSW cipher texts with just two pairings which can be achieved by length of private key by a fixed factor. It provides fast execution for decryption of data but they have also implemented the cipher text-policy based ABE scheme which incurs increased cost.

The [7] proposed the comparative analysis of performance of lightweight cryptography algorithms used in domain of RFID applications. The code analysis is performed for the cipher algorithms such as HIGHT, KATAN, TEA and KLEIN. These algorithms are then studied for their execution time by implementing them on AVR platform. The results are then formulated in desired manner.

The authors presented thorough analysis of available lightweight cryptographic algorithms in considerations of hash functions, symmetric and asymmetric algorithms [8]. The available schemes are classified and evaluated based on metrics such as efficiency and robustness. The various applications and challenges are also presented by adopting these schemes.

In [9], the XOR manipulation is used for encryption to provide privacy and faking protection instead of any other complex hash function. The security enhancement is well described and demonstrated using hardware support. The [10] proposed cryptographic method having reduced complexity and provides the intrinsic security offered by random linear network coding. This helps in reducing overheads and confidentiality is ensured by encapsulating the source coefficients that are required for decoding data, which allows intermediate nodes to perform their routine network operations.

The ECC uses digital signatures for efficient encrypting and decrypting in access booting. The generation key has a vital role in ECC [11]. ECC achieves better privacy and security compared to other cryptographic algorithms.

The [12] proposes combining symmetric and hash chain along with ECDH. The storage capacity, complexity during computation and cost of communication are efficient in protocol and also supports flexibility against the improvement of network and size of different network sensor. This is more efficient protocol than others.

The [13] presents existing lightweight schemes implementation that has less efficiency and they have high computational and communicational overhead.

The [14] carried out research or survey on existing symmetric and asymmetric protocols in IoT and proposed a Hybrid Lightweight Algorithm (HLA) that combines the properties of lightweight symmetric and asymmetric algorithms and produced a scheme that initially checks for the data size, battery threshold, memory space and computation overhead and then decides to compute either symmetric or asymmetric encryption.

Based on the related works mentioned in this paper, a Table III has been carried out to show the benefits and challenges or issues in the existing lightweight cryptographic algorithms.

TABLE III

COMPARISON OF LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS IN IOT AND THEIR BENEFITS AND ISSUES

Sr. No.	Description	Benefits	Issues/Challenges
1	Fuzzy IBE	Predefined error tolerance ability	Distance metric between identities can be a vital problem
2	New ABE with non-monotonic access structure	Less expensive, powerful to express Boolean access formula	Less efficient, complex
3	Attribute based encryption with fast decryption in PKC	Constant pairing for decryption, low key size	Time consuming
4	Efficient cipher text policy based encryption with constant size cipher text and constant computation cost	Low cost, cipher text size is efficient, scalable and simple	Constant size cipher text is challenging, computational cost overhead will be more
5	Efficient public key attribute based broadcast encryption scheme allowing arbitrary access policies	Supports complex access policies, low cost, bandwidth requirement is reduced	Does not assure attribute collusion resistance
6	Code analysis of lightweight encryption algorithms using RFID systems to improve cipher performance	Limited power supply and memory, confidentiality is attained	Time consuming, the performance may vary based on number of rounds and type of operation
7	Lightweight authentication protocol for internet of things	Reduces inadequacy, efficient and secure key establishment	Need to establish mutual authentication
8	Elliptic Curve Cryptography in context of Internet of Things	Efficient privacy and security, smaller key size	More complex and difficult to implement
9	Lightweight key establishment in WSN based on elliptic curve cryptography	Adaptable to support various size. Flexible and more efficient.	Need to optimized key size and power supply

IV. OPPORTUNITIES AND CHALLENGES IN IOT SECURITY

Based on the review carried out in this paper, there are some relevant opportunities and challenges in lightweight cryptographic algorithms designed in IoT security. They are,

A. *Opportunities:*

- There are several attacks for which the existing security solutions would be vulnerable such as Denial of Service Attack (DoS), Man-in-the-Middle, Eavesdropping, Masquerading, Saturation, Differential attacks.
- There is a huge dependency on the hardware being used for various types of communications and each hardware having different set of features and attributes on which there can be implementation of lightweight cryptography scheme that would be used upon most of the hardware resources for data transmission.
- There is a need to prevent the replay attacks on each layer of IoT security even though IoT layers provide secured protocols to prevent it. But, the data is still vulnerable to replay attacks.
- The existing security algorithms do not guarantee optimum level of security due to IoT having the broadcast and scalable nature.

B. *Challenges:*

- Due to IoT scalable nature, any node in Wireless Sensor Networks can be added dynamically will actually change the practical implementation of data transmission in real time scenarios and new nodes may get unauthorized access to the network.
- The devices are resource constrained in terms of power and bandwidth. Thus, the protection solutions on the similar can hamper the efficient working of devices.
- Lack of human interference might result in physical and logical attacks

V. CONCLUSION

The paper carried out the issues in security and privacy in Internet of Things and mainly focuses on summarizing the use of lightweight cryptographic primitives. These algorithms are specially designed for IoT networks and provide the desired level of security. The various lightweight cryptographic algorithms have been discussed and comparative analysis of the same are presented that shows the benefits and challenges/issues. The opportunities and challenges have been carried out based on these algorithms. The paper can be used as point of reference for implementing lightweight security algorithms in IoT environment.

REFERENCES

[1] European Commission, "Internet of Things – A Roadmap for Future", 2008, p. 1-32.
[2] Xue Yang,Zhihua Li1, ZhenminGeng, and Haitao Zhang, "Multi-Layer Security Model for Internet of Things", IoT Workshop 2012, CCIS 312, pp. 388-393, 2012.
[3] Amit Sahai, Brent Waters, "Fuzzy Identity based Encryption", Adv. Cryptology-EUROCRYPT 2005, pp. 457-473, 2005.
[4] RafailOstrovsky, Brent Waters, "Attribute Based Encryption with Non-Monotonic Access Strcutures", CCS'07, Proc. 14th ACM Conference on Computation, Communication and Security, October, pp. 195-203, 2007.
[5] C. Chen, Z. Zhang, and D. Feng, "Efficient Cipher-Text Policy attribute-based encryption with constant-size ciphertext and constant computation-cost.", Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6980 LNCS, pp. 84-101, 2011.
[6] S. Hohenberger and B. Waters, "Attribute based Encryption with Fast Decryption", Lect. Notes Comput. Sci., vol. 7778 LNCS, pp. 162-179, 2013.
[7]M. Alizadeh, J. Shayan, M. Zamani, and T. Khodadadi, "Code Analysis of lightweight encryption algorithms using RFID systems to improve Cipher Performance", 2012 IEEE Conf. Open Syst. ICOS, 2012.
[8] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight Cryptography for Embedded Systems – A Comparative Analysis", DPM 2013 and SETOP 2013, LNCS 8247, pp. 333-349, 2014.
[9] J. Y. Lee, W. C. Lin, and Y. H. Huang, "A Lightweight authentication protocol for Internet of Things", International Symp. Next-Generation Electronics ISNE 2014, pp. 1-2, 2014.
[10] J. P. Vilela, L. Lima, and J. Barros, "Lightweight Security for Network Coding", pp. 1750-1754, 2008.
[11] P. Shruti and R. Chandraleka, "Elliptic Curve Cryptography Security in the context of Internet of Things", vol. 8, no. 5, pp. 90-93, 2017.
[12] S. Ju, "A Lightweight ket establishment in wireless sensor networks based on elliptic curve cryptography", IEEE conference on Intelligent Control, Automatic Detection and High-End Equipment (ICADE), pp. 138-141, 27-29 July, 2012.
[13] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute based encryption scheme for the Internet of Things", Future Generation Computer Systems, vol 49, pp. 104-112, 2015.
[14] Saurabh Singh, Pradip Kumar Sharma, SeoYeon Moon, Jong Hyuk Park, "Advanced Lightweight Encryption Algorithms for IoT Devices : Survey, Challenges and Solutions", J Ambient Intell Human Comput., 2017.
[15] S. Chandra, S. Bhattacharya, S. Paira, Sk. S. Alam, "A Study and Analysis on Symmetric Cryptography", International Conference on Science, Engineering and Management Research (ICSEMR), 2014