LIGHT WEIGHT CRYPTOGRAPHY AND HOMOMORPHIC ENCRYPTION FOR IOT

Rafidha Rehiman K A[1], *Dr. S Veni* [2]

ABSTRACT

Cryptographic techniques like AES are available for offering better security, but the current implementa tions are not adequate enough to support the constrained architecture. This work is a study of the requirement of Light Weight Cryptography and a combined authentication and confidential scheme for IoT. A comparative analysis and the requirement of homomorphic encryption for centralized storage have also been carried out. The homomorphic encryption has proved its advancement and applicability in the sensor world. Homomorphic encryption is valuable for automatic sensor environment, but in a constrained system like IoT, an optimized method for homomorphic implementation is required.

Keywords : cryptography, light weight, internet of things, IoT big data

I. INTRODUCTION

Cryptography supports secure communication over the internet by ensuring data confidentiality, integrity and availability. Different symmetric and asymmetric algorithms are available to restrict unauthorized access and use of protected resources.

Cryptography transforms any information from source called plaintext to a scrambled format by means of some mathematical procedures and a key. Depending on the nature of the key, cryptography is divided into symmetric key cryptography and asymmetric key cryptography. If a single key is used for transformation and recovery, then the key is known as symmetric key. On the other hand, two different keys are used for encryption and decryption, and it is called the public key cryptography. The basic classification of cryptology is shown in figure 1.

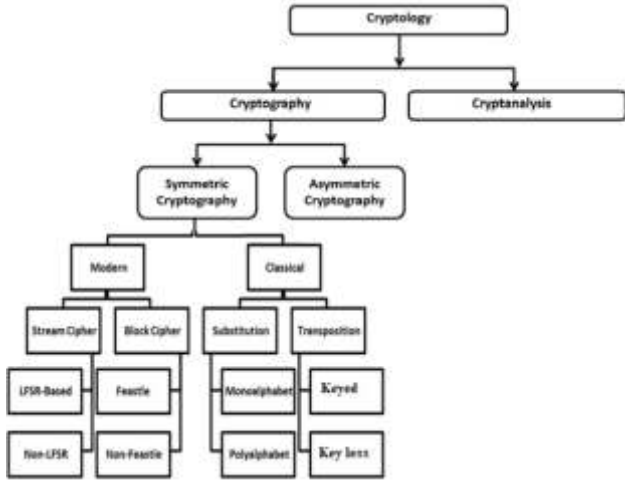

Figure 1: Classification of cryptography

Cryptographic algorithms are said to be effective, if they are able to provide security and if it is implemented in an economical way. The security offered by a cryptographic algorithm depends on key value, its length, the procedure followed to generate keys for

[1] Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education Coimbatore.

[2] Associate Professor & Head, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore.

different rounds involved and the block size, if block cipher.

After the design and implementation of the cryptographic algorithms, it is necessary to prove that the implementation of the algorithm is resistant to cryptanalysis. Mainly cryptographic algorithms are classified as computationally secure cipher and unconditionally secure cipher. In case of computationally secure cipher, an analyst is required to make more effort, and the cost will be more than the value of the information. The vulnerabilities may arise in these systems any time. An unconditionally secure cipher does not reveal any information about the plain text. A cryptographic algorithm is considered to be secure, if it is able to provide more security. It is possible to enhance the security of cryptographic algorithms by combining multiple systems to form a hybrid system [1].

Some of the modern block ciphers such as DES, 3DES, CAST, BLOWFISH, etc. involve multiple key mixing, expansion, substitution and permutation functions to provide secrecy. DES is vulnerable to exhaustive key search attack because of the 56 bit key used, and suffers from weak key and semi-weak key problems. BLOWFISH algorithm is also a feistel structure cipher similar to DES, and requires more processing time with the supporting variable-sized key value.

CAST offers more resistance to linear and differential cryptanalysis, but is vulnerable to chosen plaintext attack. AES offers higher security and is under the category of computationally secure cipher. Different types of attacks are tried on AES but it can withstand these attacks. AES is an algorithm which offers better security, but the requirements for execution are not acceptable in a constrained infrastructure. Thus, it is better to rewrite the algorithm to reduce the resource consumption without compromising efficiency.

Public key cryptosystems are computationally secure, and security is entirely based on integer factorization problem and discrete logarithmic problem. Factoring the public key n used in RSA, it is a tedious and time consuming work and the cost of breaking the cipher will definitely exceed the value of the information.

Different software implementations of cryptographic algorithms exist in literature and no one has benchmarked the fastest algorithm by implementation [2]. We are able to speed up the execution of algorithms using modern multicore and graphical processing units.

Internet of Things is an emerging revolution in which different objects automatically participate in the communication. The participation forms a decentralized network and is very hard to identify the device operating in a particular perimeter. The security and protection of both the information and the devices are a major concern and need to be addressed by the research community[3]. IoT facilitates users to access and share information and make decisions, but is susceptible to different kinds of attacks. The attacks encountered in IoT environment are: Denial of Service, eavesdropping, Alteration, Fabrication etc. Also, any malfunctioning device in a trusted network exploits the entire system, and therefore security implementation is a prime requirement [4]. Preventing leakage of information from a secure environment is a major challenge in IoT. Applying the encryption on tiny devices is only a counter measure against threat to confidentiality, but we need protection at application layer.

Advanced cryptographic technologies and software

implementations are mainly concentrating on high end work stations, not suitable for battery powered IoT devices. The memory and other resources required for the execution of modern cryptography algorithms do not take into consideration the constrained environment.

II. LIGHT WEIGHT CRYPTOGRAPHY

Light Weight cryptography is an expansion of cryptography aiming at low memory requirements and computational complexity. The main intention of designing light weight algorithms is to make it run on the devices with little computational requirements. Light weight cryptography is divided into ultra-light weight and ubiquitous cryptography [5][6].

Light weight cryptography, based on the performance in terms of resource requirement, offers cost effective security. Now, the light weight cryptography is reactivated within the fastest growing M2M/IoT world. With the high popularity of IoT, NIST announced a public call for applications to light weight cryptography in 2017.

Usually Light weight algorithms are designed keeping AES as standard, because AES is standardized by NIST. In IoT the expected authenticated encryption is AES CCM or GCM. AES is faster than TWINE, if the available ROM is greater, than or equal to, 1KB. Table 1 concludes the existing light weight algorithms available in literature.

The factors which address the requirement of light weight cryptography are characteristics of IoT devices. The researchers need to consider the size, processing power and power consumption of the devices operated in a wireless sensor network. Another big challenge in this area is to address all the goals namely confidentiality, integrity and availability.

The key aspects to be kept in mind while developing security solutions for constrained environment include:

1. Use of existing security solutions for securing the applications in a constrained environment.
2. Modifying the existing well-secured solutions for conserving the usage of resources and battery power of the portable devices without compromising on security.
3. Developing new innovative solutions for a constrained environment so as to secure data and resources.

Algorithm	Structure	Block Size	Key Size	Analysis
PRESENT	SPN	64	80/128	Hardware efficient. Require large processing.
RECTANGLE	SPN	64	80/128	Hardware efficient. Software efficient.
HIGHT	FIESTEL	64	128	Ultra Light Weight High Security
CLEFIA	FIESTEL	64	128/192/256	Good hardware performance
CAMELLIA	FIESTEL	128	128/192/256	Comparable to AES Part of TLS
TWINE	FIESTEL	64	80/128	Implemented in small circuitry. Passed CAESAR
SIMON	FIESTEL	128	128	Small amount of ROM Power efficient Optimized performance
SPECK	ARX	Variety of Block size	Variety of key size	Optimized Software performance
OTR	2R FIESTEL	2 variants TWINE OTR AES OTR		Passed CAESAR Authenticated encryption
Humming Bird	Stream-Block Cipher	16	256	Suitable for smart cards

Table 1: Comparison of light weight algorithms

Among the light weight algorithms HIGHT is designed to be used in Wireless sensor networks 8 bit computing devices. HIGHT uses bit by bit XOR operation for speed optimization and battery driven devices[18].

RC5, TEA and XTEA are also under the category of Light weight algorithms and are suitable for constrained environments. Almost all the available implementations are based on symmetric key cryptography, because they are faster than asymmetric key systems, and guarantee confidentiality. The computational complexity of public key systems is 1000 times higher than that of private key system.

To address issues related to the ownership of data, a light weight signature mechanism supporting asymmetric cryptography is a must in IoT. One of the main advantages of these public key mechanisms is the offer of all security services. Also, the systems forced to communicate with dynamic parties/devices need light weight encryption methods relying on public key cryptography to offer all benefits [7][8].

Chowdhury, Amritha Roy, Tanusree Chatterjee, and Sipradsbit has proposed a light weight authentication scheme "LOCHA" based on light weight hash function, used for WSN. The scheme uses MOD and SWAP functions to make it low overhead [19].

SLES is a simple light weight encryption scheme based on pseudo-random bit sequence generated by using elliptic curve cryptography. The plain text message is converted to a bit stream and XOR with the sequence generated to prepare the cipher text. The scheme is suitable for large volume of data.

Various algorithms are surveyed and an identity-based hashing scheme is proposed based on elliptic curve cryptography to support both authentication and confidentiality in constrained environment.

III. HOMOMORPHIC ENCRYPTION

Now Internet of Things (IoT) is the most widely used interaction paradigm in the smart world. Security is a prime requirement and a major challenge in IoT data analytics and storage. The number of devices with sensing and communication capabilities connected to the Internet has increased to billions and pulled out huge volumes of data. All of the IoT functionalities are either implanted or wearable, and are always with users to pull out sensitive private information. Cryptographic algorithms protect our sensitive data from unauthorized access and usage [9] [10].

The most important feature of IoT is sensor-collected private information and real time or close to real time communication. Modern cryptography permits computations on encrypted information, and hence after reviewing the works available on literature, we propose an ECC based homomorphic encryption for sensor data in IoT environment for privacy preservation. There are white spots in which data are available in a plain text format, when moved from one environment to another [11]. In storage, the encrypted content is decrypted, analyzed and information gathered, and so there are chances for the availability of sensitive information in clear format in intermediary nodes and storages. When data are decrypted for operations and computations, an adversary can capture it and use it for some malicious purpose. Also, a malfunctioning or vulnerable node can steal private sensitive data. This raises the privacy challenges in IoT eco systems.

Storing data in a more secure private cloud is more

expensive than storing it in a public cloud Internet. Internet cloud allows us to use applications for our computations without installing the software on the processing environment or personal computer. The users are unaware of where actually the source of application is and where to move the data, and the results obtained after processing by these applications. Some cloud sells the private sensitive information for financial gain.

To avoid the difficulties associated with computations and operations on plain text data in intermediary storage or workstations, we require a method for processing on encrypted data. The operations carried on encrypted information should be without any knowledge on the plain text and the encryptions applied on it.

Homomorphic encryption is an application of Public Key Cryptography and this method allows us to perform computational operations on encrypted data. For ensuring the security of IoT data and to protect it while in transit, we implement a light weight ECC based method along with compression [12]. The encryption protects the data until decryption, but to preserve privacy and maintain anonymity Homomorphic encryption is suitable. The method performs computations on cipher text without decrypting it, and the owner is able to recover the exact information from the processed cipher text. Also, result obtained will be same as the result of computations from the plain text.

A. Related Works

The concept of Homomorphic encryption was first introduced by Rivest, Adleman and Dertouzous in 1978[13] and has remained untouched to date. For homomorphic encryption first, the owner of data generates the key values for secure communication. He encrypts the data with a public key and sends the encrypted data with his ID to the centralized cloud storage. The storage then processes the encrypted information without decrypting the cipher text. The results of computations are required to be passed to the owner to decrypt. Thus, only owner is able to understand the information and can maintain the secrecy in public storage.

An encryption scheme is said to be homomorphic, if we have Cipher Text C1 = Encryption (Plain Text P1) and C2 = Encryption (Plain Text P2) and if possible to compute Encryption (F(C1 and C2)), where F is the function and may be Addition, Multiplication or Exclusive OR, the operation is carried out without knowing the decryption key of corresponding encryption .

Shaffi Goldwasser et al proposed an additive homomorphic system for single bit encryption. Then Dan Bonch came up with a system for multiple additions and a single multiplication operation [14]. Recently RSA and Elgamal based schemes proved as multiplicatively homomorphic for encrypted processing.

Several homomorphic schemes are available like Paillier, RSA, Elgamal, BGV, EHC etc. CryptoDB is the first practical homomorphic mechanism made available in literature for encrypted query processing in DBMS [15]. This method processes the operation and queries on the encrypted content saved on data base, and using storage and computation expensive cryptographic techniques ensures protection. The method is not practical in IoT environments .

Hossein Shafag et al 's 'Talos', an IoT data protection system securely stores encrypted data on cloud and allows the processing on encrypted data by considering data producing systems and leaves data consuming system for the future.

The recent researches on homomorphic encryption have proved their advancement and applicability in the sensor world. For the constrained IoT we require an optimized method for homomorphic implementation. The conventional solutions are affordable in cloud but not practical for the other end devices.

B. Big data and IoT

In the years to come, we will have billions of interconnected devices and Big data pulled out from these devices. Traditional Data Base Management Systems are not suitable to capture, store or analyse large volumes of data. We require advanced analytics for sensor-collected IoT data, and thus we can combine big data and IoT technologies to improve the functionalities and operations of various sectors.

We have reasons for the requirement of combining technologies. Because Iot generates big data, data need to be analysed for information, and this will improve the performance of devices. There are challenges in extracting and using data collected by the IoT sensors. Also, Big data analytics in IoT introduces new challenges in Data Security. We have mechanisms to protect our data in storage, but they are very slow when applied to massive volumes.

The rate of growth of data expands every second; so, storage is a huge challenge. The devices operated in a cloud environment suffer from insecure computations in distributed environment, insecure transactions and insecure access controls. A fast secure encryption technique and multilayer security system are a required for real time processing in Big data.

In IoT cloud storage, sensitive information can reside anywhere and can lead to privacy violation which risk our data. Cloud encryption is a solution to ensure privacy and sensitivity. If data are stored as encrypted text, another challenge faced is query processing in encrypted data, as the entire data are required to be decrypted for processing a query for match finding. This will take a significant amount of time and the process becomes slower. There is scope for Iot in the area, and the problem of Big data security, as a majority of security related problems, is still unsolved and needs to be considered [16][17].

IV. CONCLUSION

This paper provides an analysis of various cryptographic algorithms. Asymmetric algorithms are more secure than symmetric algorithms. The goal of this analysis is to point out the requirement of Light weight cryptography for a constrained environment. With light weight cryptography we can provide a moderate level of security to data and information. Homomorphic encryption is really valuable for automatic sensor environment, but in the constrained IoT we require an optimized method for homomorphic implementation. The conventional solutions are affordable in cloud but not practical for the other end devices. An ECC based homomorphic encryption is proposed for IoT to perform computations on encrypted data.

REFERENCES

[1] Zoran Hercigonja, Druga gimnazija, Varaždin, "Comparative Analysis of Cryptographic Algorithms," International Journal of DIGITAL

TECHNOLOGY & ECONOMY,Vol 1, No2, 2016.

[2] Vladislav Nazaruk, Pavel Rusakov "Implementation of Cryptographic Algorithms in Software: An Analysis of the Effectiveness", Scientific Journal of Riga Technical University Computer Science. Applied Computer Systems, Vol43, 2010.

[3] Ikram Ud Din et al, "Trust Management Techniques for the Internet of Things: A Su rvey", IEEE Access· November 2018.

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

[5] Isha Bhardwaj, Ajay Kumar, Manu Bansal, "A Review on Light Weight Cryptography algorithms for data security and and authentication in IoTs", IEEE international conference on Signal processing computing and control, 2017. Daniel Engels2

[6] Xinxin Fan, Guang Gong ,Honggang Hu, Eric M. Smith, "Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices", Lecture Notes in Computer Science, 2010.

[7] Kazuhiko Minematsu, Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions

[8] Okamura Toshihiko, "Light weight cryptography applicable to various IoT devices", NEC technical journal/Vol 12/no1/ Special issue on IoT supports digital business.

[9] William Stallings ,"Cryptography and Network Security - Principles and Practice", Pearson, 2016

[10] Behrouz A. Forouzan, "Cryptography & Network Security ", McGraw-Hill 2007.

[11] Tyler Wrightson, "Hacking exposed Wireless Network Security A Beginner's Guide", 1st Edition, Tata Mc - Graw Hill, 2012. Lee, Hyungjick,jim Alves-Foss, Scott Harrison, "The use of encrypted functions for mobile agent security", Hawaii international conference, IEEE 2004, pp 10-15.

[12] Lee, Hyungjick,jim Alves-Foss, Scott Harrison, "The use of encrypted functions for mobile agent security", Hawaii international conference, IEEE 2004, pp 10-15.

[13] Rivest Ronald L, Len Adleman, Michael L Dertouzos, "On data banks and privacy homomorphism", foundation of secure computation4 no.11(1978) 169-180.

[14] Payal V Parma etal, "Survey of various homomorphic encryption algorithms and schemes", International journal of computer applications, vol 91, April 2014.

[15] Hossein Shafagh et al, "Talos : Encrypted query processing for internet of things", ACM 978.

[16] Raghav et al, "Big Data Security issues and Challenges", International Journal of Innovative research in advanced Engineering, issue2, vol 2 , ISSN 2349 - 2163, 2015.

[17] KR Kundhavai, S Sridevi, "IoT and Bigdata - The current and future technologies : A Review",

International Journal of Computer Science and Mobile Computing, vol5. Issue 1, 2016.

[18] Koo et al, "Implementation and analysis of new light weight cryptographic algorithm suitable for wireless sensor networks", Information seccurity and assurance 2008, IEEE.

[19] Chowdhury, Amritha Roy, Tanusree Chatterjee, Sipradsbit , "LOCHA : A light weight one way cryptographic hash algorithm for wireless sensor network", Procedia Computer science 32, PP, 497-502, 2014,

[20] Biswas, Kamanashis, Vallipuram Muthukumaraswamy, Elankayarsithirasenan kalvinder singh, "A simple light weight encryption scheme for wireless sensor network", Springer 2014.