6th International Conference on Research Developments in Applied Science, Engineering & Management
Mahratta Chamber of Commerce, Industries and Agriculture, Pune (India)
23rd March 2019 www.conferenceworld.in
Conference World
ISBN : 978-93-87793-78-1

A COMPREHENSIVE ANALYSIS OF LIGHTWEIGHT CRYPTOGRAPHY FOR IOT-SECURITY

Khushnuma [1], **Mrs. Priyanka Agrawal** [2]

[1]*Electronics & Communication Engineering Department, Jaipur Institute of Technology, Jaipur*

[2]*Asst. Prof. of ECE, Jaipur Institute of Technology, Jaipur*

[1]Khushisiddiqi2014@gmail.com [2] Priyankaagr.er@gmail.com

ABSTRACT:

Internet of things is abbreviated as IOT. Today IOT is a key and overriding subject of the technical and social significance. Products of consumers, items and vehicles, industry based and basic components, sensors, and other day to day objects are merged with connectivity of internet and the strong data capabilities which assure to change the type in which we work and live. The influence of the devices based on the Internet and economy are attractive, with some 100 billion devices connected to IOT and a worldwide economic impact of mostly $11 trillion by 2025.The concept of mixing computers, the sensors, and networks to specifically command the devices that is existing for numerous years. The technology for this process includes similar connectivity, huge and wide adoption of IP-based networking, calculating the economics, minimizing the size of the devices, highly advanced data analytics and the cloud computing.Internet of things has already made the things easy to use and easy to access, it involves the ability to transfer data directly to the network. The main problem is that security is always a threat in product design. To improve the security of the IOT devices that are directly accessible over the internet work over the world is in progress. The motivation of the work is to protect the devices from the security threats and to improve the security of the devices which are directly accessible to the internet as today the dependency on IOT is increasing and if people need to use IOT they must have the security for their devices and data that is directly accessible through internet.

I. INTRODUCTION

As the number of IOT devices are growing in the society, then the amount of traffic generated by them obviously rise significantly. Networking and communication models for the objects consist of those where the interchanged data does not inter cross an IP-based network. The data generated from the objects which are IOT based will pass over gateways with the connectivity to IP-based networks or will be accessible through the Internet. The users of IOT devices are more merged with the services delivered and used where data passes over IP-based network. Despite in today's world everyone is concerned about IOT and IOT is emerging as a very popular technology yet we don't have a specific and a particular definition of IOT. According to different books all over the internet of things is defined as thegroup of many embedded devices which are processed over internet via some IP protocols. This system allows the devices to exchange the data over the network and these

ISBN : 978-93-87793-78-1

devices are or accessible by the humans. Internet of things have become very popular and some of its uses are listed as a few examples like it is used to monitor the health of the human body via a device which is attached to the human body or is attached inside the human body and these devices then gives the information about the human health and care. IOT consists of the systems which monitors the security of the buildings. The IOT devices are used in stores, banks, offices and arenas and in energy management and security of these official buildings. The IOT devices are also used in factories, worksites and vehicles and for the maintenance in navigations also the IOT system networks are used. All of the definitions described in the society explains the scenarios in which network connectivity extends to a celebration of objects, devices, sensors, and everyday objects that are not ordinarily considered to be "computers''; this allows the devices to generate, exchange, and consume the data, often with minimal human interference. The various definitions of IOT do not actually disagree either it focuses on different indulgence of the IOT phenomenon from different points and use cases. [7]

There are four major frameworks which are present over here and the following section explains about the key characteristics of each model in framework, the models described by framework are listed below:

- Device to Device communication
- Device to cloud communication
- Device to gateway model
- Back end data sharing model

II. LIGHT WEIGHT CRYPTOGRAPHY FOR IOT

Light weight cryptography refers to the type of encryption and decryption which includes less power, size and memory consumption. The basis of light weight cryptography is low cost and minimal size. Now we have terms like size of the key, number of encryption rounds, cost which are directly related to the performance of the algorithm. If we need toachieve a design which is cost effective, good in performance and also minimum in size than this task would be difficult. For instance if we try to implement this type of algorithm than it would require a huge area which results in high cost, and if we need to achieve a design with high reliability and of minimum cost than we need to compromise with the capacity. Among all there is a basic component which is used for the light weight cryptography that is GE gate equivalent. This defines about the production's complexity. GE plays an important role in the field of hardware implementations. In today's era we are in a need of hardware implementations too which demands less number of GE. Most of the algorithms used today are a part of software without hardware usage. Due to this the already existing algorithms are impossible to implement on the devices which are having a limited processing power, less volume and the less amount of power consumption. The basis of the light weight cryptography is the reduction in cost for overall process. The developers of this type of cryptosystem have to focus on the performance, cost and the security. Yet all the three aspects can't be given an ideal shape for the development of an algorithm but yes the researchers are still working on this to get

ISBN : 978-93-87793-78-1

almost an ideal algorithm for the IOT devices which are again the wireless self made network between the items of the different environment which includes the home appliances to the outer world devices. The up grown approaches yet are trying to solve the cost issues and are creating the methods to understand the cryptosystem and its necessities some of these can be the usage of the traditional cryptographic protocols, modification of the previously used algorithms on the basis of hardware implementations, cost and limitations and the emergence of modification in the methodology to generate the algorithm The aim is to get a reliable and cost effective system. The chip area is limited and that should be implemented for getting the cost effective algorithm, it is also important to take care about the type of circuit if it is active or passive. The main focus is on the reduction of size of the encryption key, block encrypted data and the algorithms internal state, which is why the algorithm would become light weight.[12,13,20]

III. SURVEY ON LIGHTWEIGHT CRYPTOGRAPHY

The methodology used for developing the algorithm Some of the terms important to know while considering the light weight cryptography and studying the light weight cryptography are described below in detail:***Light Weight Cryptographic Primitive-***

From the past decade, large number of lightweight cipher primitives has been introduced, which consist of the block ciphers, hash function, authentication codes of messages, and stream ciphers, they provide advantage in performance above the traditional cryptographic methods. These primitives are different from the existing algorithms in which the lightweight primitives are not compatible for a large number of applications and can limit the capabilities of the attacker. For instance, the attacker can have a very limited amount of data available at a single key. However, it should not be misunderstood that lightweight algorithms are weak the basic aim is to use advance technology, which gives a way to better design security, good performance and resource requirements in a particular resource balanced environment.[16]

Lightweight Block Ciphers-Advanced Encryption Standards has proposed the various number of lightweight block cipher to get great advantages in the field of performance. There are some passwords which are designed to improve the efficiency by making it simple in the good traditional analysis block cipher. FOR example DESL is an advance version of DES, in this we do not require eight S boxes instead of that a single circular function is required and it deletes the initial and final permutation to make the size of the hardware much better, opposite to this some unique block cipher algorithms are designed to get started from the head. PRESENT (algorithm) is one of the first lightweight block cipher design proposed to use in the tough hardware surroundings. SIMON and SPECK these algorithms are the members of family of lightweight block ciphers that are simple to design are flexible, and perform very well on hardware and software both. There are many algorithms such as RC5, TEA and XTEA, which make a simple circular structure and make itself suitable for harsh software environment. If we compare with the traditional block ciphers, the advantage of lightweight block ciphers is achieved via lightweight design options like:[22][21][19]

ISBN : 978-93-87793-78-1

Smaller block size: To save the memory space, lightweight block ciphers uses much smaller block size than AES. If we use a small block size than that will reduce most of the number of plaintext blocks which are to be encrypted. For instance, for some type of approved operations, the result of a 64-bit block cipher may differ from the random sequence which uses almost 232 blocks. Now whatever algorithm we are using it depends that the attackssuch as plaintext recovery or key recovery can get non-negligible probabilities.

Smaller key size:Some lightweight block ciphers use smaller keys which are less than 96 bits due efficiency improves. The minimum key size required by NIST is 112 bits till it has been worked now. Using the smaller key size we can improve the efficiency of the algorithm but that too has some limitations.[19]

Simple rounds:The parts and the operations which are used in the lightweight block ciphers are much simpler than the previously used block ciphers. The 4 S-Box is much more popular than the 8 S-Box in the lightweight designs which are using S-boxes. The reduction in this size leads to a great significant saving in terms of memory, space etc. Like if we talk about the 4-digit S box used in the algorithm PRESENT that requires 28 gates, and of the same algorithm AESS box needed 395 GE. For the hardware-based design little more arrangements used in algorithms or reoccurring MDS matrices like PHOTON and LED can perform over linear layers. When the encryption round is easy and simple it is necessary to repeat it more times to maintain security.[2][6]

Simpler key schedules:If we use the complex key schedules then we can face the reduction of their importance, concealment, and the usage of power consumption; so most of the lightweight block ciphers use a very simple key which can generate simpler keys on the processor. This can utilize the exact key, it can be a weak key, any known key or even it can be a selected key to attack. Using security key derivation (KDF) it is possible to avoid some of these kinds of attacks.[11]

Minimal implementations: There are many types of operations and protocols which exactly require the encryption of the block cipher. In many of the applications it is required that device supports only one encryption or decryption method operations. Rather we implement the whole password we can apply only the necessary features of a password because it will require a very few sources of error, rather than that of applying the whole of it.

Lightweight Hash Functions:Previously used hash functions not necessarily are suitable for the harsh and the tough environments, especially due to the large internal state and very high power consumption requirements which basically path towards the development of lightweight hash functions such as PHOTON, Quark, SPONGENTand Lesamnta-LW etc. The use expected for the regular and lightweight hash functions are different in the different aspects of the surroundings. This can be seen in the following sections:[22][18]

Smaller internal state and the output sizes: Hash functions that are required by the larger output sizes are important for anti-collision applications. The applications which do not require anti-collision, smaller internal

ISBN : 978-93-87793-78-1

states and output sizes are used. If it becomes necessary to use an anti-collision hash function, it is accepted that the hash function which has the same security for the pre-image, the secondary image, and even for the collision attacks. This practice can reduce the size of the internal state.

Smaller message size: Traditional hash functions are expected to support the inputs with very large sizes(around2^64 bits).In most of the protocols for light weight hash functions that are targeted the typical input size is much smaller than the conventional size (almost256bits).Hash functions which are kept for short messages can therefore be better for the lightweight applications in the IOT devices.

IV. SYMMETRIC LIGHTWEIGHT ALGORITHMS FOR IOT

Advanced Encryption Standard (AES): This is mainly used as a built-in solution for application-layer COAP. NIST has standardized this symmetric block cipher which uses a permutation network and operates with a 4×4 matrix which has a length of 128 bits. Each and every bite is mainly affected by the following sub bytes, the shifted rows, and the mixed columns. The key size can be of 128-bit, 192-bit and 256-bit.The protocol AES is still a savior to the man-in-the-middle attacks.

High Security and HIGHT: It uses a very basic operation like addition and it adds mod 28 or XOR to work with the Feistel network. It consists of a 64-bit block size and also works on 32 rounds over a 128-bit key. The key of this algorithm is generated while the encryption and decryption process is going on. A highly parallel implementation requires very less energy, is mentioned with several lines of code, and it also increases the speed of the RFID system. HIGHT is open to the saturation attacks.

Small Encryption Algorithm (TEA):TEA is used in the environments which are very much restricted like sensor networks and the era of smart objects, it can be explained and jotted down in minimal amount of lines and it is restricted to be very simple and need not to be tough to be executed and to be explained. It uses block sizes of 64-bit and 128-bit keys, also it donot use the already calculated tables or any of the predefined calculations for the results. There are number of various versions of TEA, like extended TEA19, block TEA. These extensions work to solve the drawbacks in the original TEA. However, due to its simple operation, TEA and its extensions are very much prone to multiple attacks.

• *PRESENT*: This algorithm is based on SPN and is seen an ultra-lightweight algorithm for security purpose. It is suitable for the hardware optimization in the alternative layers by using 4-bit input and output S-boxes. It has a key size of 80 or 128 bits and it operates on 64-bit block. PRESENT is been proposed as a lightweight cryptographic solution in ISO/IEC 29192-2:2012 “Lightweight cryptography”. [2]

• *RC5:*This is the first data-independent rotation algorithm which was presented by Rivet. It has a Feistel structure which works perfectly as the lightweight algorithms which are being used in wireless sensor networks. RC5 is also known in the form of w / r / b, where w is the size of the word, r is the number of working cycles,

and b will tell the number of bytes of the encryption key. RC5 generally works on 32-bit size, but the variants can be 16, 32, and 64. It can use 0 to 255 bytes to work 0 to 255 rounds. It uses the standard key size is 16 bytes in 20 rounds of operation. RC5 is prone to the differential attacks.[9][6]

The "Lightweight Cryptography", in the IOT is very advantageous there are two reasons that supports the usage of light weight cryptography the first is efficiency of end-to-end communication to achieve some end-to-end security, end nodes implement the symmetric key algorithm for the purpose of security. For the low resource-devices like battery-powered devices, the cryptographic issues with very low amount of energy consumption are a must. Due to lightweight symmetric key algorithm lower energy consumption for end devices is applicable. Applicability to lower the resource devices the footprint of the lightweight cryptographic primitives is much smaller than the traditional cryptographic algorithms. The lightweight cryptographic primitives would give the possibilities of larger network connections with less resource devices. However, the minimal cost devices can get into the application-specific ICs because of the limited cost and minimum power consumption, when the hardware properties are very important, due to the fact that most of the already in use algorithms cant be used in the places where we talk about only the optimization of the software specially when we are heading towards the light weight cryptography. Most of the algorithmsused today as a part of software without the hardware usage. Due to this the already existing algorithms are impossible to implement on the devices which are having a limited processing power, less volume and the less amount of power consumption. The basis of the light weight cryptography is the reduction in cost for overall process. The developers of this type of cryptosystem have to focus on the performance, cost and the security. Yet all the three aspects can't be given an ideal shape for the development of an algorithm but yes the researchers are still working on this to get almost an ideal algorithm for the IOT devices which are again the wireless self made network between the items of the different environment which includes the home appliances to the outer world devices. Each and every approach has some or the other limitations, it can also be seen that if we are using these algorithms to be implemented upon hardware with its inbuilt features than this would result in the weakening of the security purpose for which the algorithm is actually meant for. The aim is to get a reliable and cost effective system. The chip area is limited and that should be implemented for getting the cost effective algorithm, it is also important to take care about the type of circuit if it is active or passive. The main focus is on the reduction of size of the encryption key, block encrypted data and the algorithms internal state, which is why the algorithm would become light weight. One of the concepts to design the algorithm in light weight concept is GE- gate equivalent. This is to measure the complexity of the technology proposed. [13]17]

V. RESULTS

Most of the algorithms used today as a part of software without the hardware usage. Due to this the already existing algorithms are impossible to implement on the devices which are having a limited processing power, less volume and the less amount of power consumption. The basis of the light weight cryptography is the reduction in cost for overall process. The developers of this type of cryptosystem have to focus on the

ISBN : 978-93-87793-78-1

performance, cost and the security. Yet all the three aspects can't be given an ideal shape for the development of an algorithm but yes the researchers are still working on this to get almost an ideal algorithm for the IOT devices which are again the wireless self made network between the items of the different environment which includes the home appliances to the outer world devices. The up grown approaches yet are trying to solve the cost issues and are creating the methods to understand the cryptosystem and its necessities some of these can be the usage of the traditional cryptographic protocols, modification of the previously used algorithms on thebasis of hardware implementations, cost and limitations and the emergence of modification in the methodology to generate the algorithm. Each and every approach has some or the other limitations, it can also be seen that if we are using these algorithms to be implemented upon hardware with its inbuilt features than this would result in the weakening of the security purpose for which the algorithm is actually meant for. The aim is to get a reliable and cost effective system. The chip area is limited and that should be implemented for getting the cost effective algorithm, it is also important to take care about the type of circuit if it is active or passive. The main focus is on the reduction of size of the encryption key, block encrypted data and the algorithms internal state, which is why the algorithm would become light weight. One of the concepts to design the algorithm in light weight concept is GE- gate equivalent. This is to measure the complexity of the technology proposed.

Advantages

- It requires very low quantity for resources and power consumption due to which it is categorize as light weight.
- Due to its light weight property these algorithms are very fast in nature and are accepted by the environment.
- The lightweight algorithms are hence very inexpensive in nature and are used easily.

Disadvantages:

- These algorithms do not have a high bandwidth which is a huge drawback.
- The currently existing algorithms which uses less GE are more usable to hardware implementations and not to the software.
- For security purpose if we increase the key length then we need to increase the number of gate equivalents which is not good for cost as well as for size.
- The increasing number of attacks on some of the very used algorithms makes the use of these light weight algorithms difficult.

V. CONCLUSION

Since the idea of combining computers, sensors, and networks to judge and control devices has been there for many decades, the current flow of key technology and the market trends is indulging in anew reality of the "Internet of Things''. IOT promises to follow up a revolutionary, fully interconnected and world, with relationship between different objects and their surroundings and objects with people becoming more closely connected. The idea of the Internet of Things as an array of devices which are related to the Internet might fundamentally change about what people think to be "online".

Even the potentials are significant, a large number of challenges stand in the path of the vision – basically in the areas of security; privacy; interoperability and the standards; legal and rights issues; and this includes the emerging economies. The Internet of Things is very famous now, and so there is a need to accept and resolve its challenges and try to maximize its benefits simultaneously reducing the risks.

Internet Society thinks about IOT as it represents a growing platform for people and institutions which can interact with each other and indulge on to the Internet and network connectivity into their personal, social, and economic lives. Solutions for maximizing the best usage of IOT with minimizing the risks can't be met by getting involved in a polarized debate that puts the promises of IOT against security threats. But it would take dedicated engagement and collaboration among the researchers and the developers to make this way towards security works.

REFERENCES

[1] Maria Almulhim, Noor Zaman, "Proposing secure and the lightweight authentication scheme for IOT based E health applications" *International* conference on advance communication technology; 2018.

[2] Muhammad NaveedAman, KeeChaing Chua, "A light weight mutual authentication protocol for IOT system,2017.

[3] Mehdi Baahrami, Dong Li, MukeshSinghal, "Efficient parallel implementation of light weight data privacy method for cloud users; seventh international workshop on data intensive computing in clouds, 2016.

[4] Gaurav Bansod, AbhijitPatil, "An Ultra light weight design for security in pervasive computing" IEEE second international conference on big data security cloud, 2016.

[5] ZahidMahmood, HuanshengNing, "Light weight two level session key management for end user authentication in internet of things" IEEE international conference on IOT, 2016.

[6] Ayaz Hassan moon, Ummer Iqbal, "Light weight authentication framework for WSN" International conference on Electrical, Electronics and Optimization techniques, 2016.

[7] Muhammad Usman, Irfan Ahmed, Shujaat khan, "SIT: A light weight encryption algorithm for secure internet of things," international Journal of advanced computer science and applications, vol. 8, no.1, 2017.

[8] D Jamuna Rani, "Light weight cryptographic algorithm for medical internet of things", Online international conference on Green Engineering and Technology, 2016.

[9] SudhirSatpathy, Sanu Mathew, "Ultra low energy security circuits for IOT applications", IEEE 34th international conference on computer design, 2016.

[10] SainandanBayyaVankata, PrabhkarYellai, " A new light weight transport method for secured transmission of data for IOT", international journal of electrical, electronic engineering, 2016.

[11] Amber Sultan, Xuelin Yang, "Physical layer data encryption using chaotic constellation rotation in OFDM-PON" Proceedings of 15th international Bhurban conference on applied science and technology Islamabad Pakistan, 2018.

[12] Xuelin Yang, ZanweiShen, "Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen plaintext attacks", in ICTON 2016.

[13] Han Chen, Xuelin Yang, "Physical layer OFDM data encryption using chaotic ZCMT precoding matrix", IEEE, ICTON 2017.

[14] GaoBaojian, LuoYongling, HouAiqin, "New physical layer encryption algorithm based on DFT-S-OFDM system" International Conference on Mechatronic Sciences, Electric Engineering and Computer, Shenyang, China, 2013.

[15] Meihua Bi, Xiaosong Fu, "A key space enhanced Chaotic encryption scheme for physical layer security in OFDM-PON", IEEE photonics Journel", 2017.

[16] Pan Cao, Xiaofeng Hu, Jiayang Wu, "Physical layer encryption in OFDM-PON employing time variable keys from ONUs, IEEE photonics journal, 2 April 2014.

[17] Amber Sultan, Xuelin Yang, "Chotic Constellation Mapping for Physical Layer DataEncryption in OFDM-PON, IEEE Photonics Technology, vol.30, no.4, 2018.

[18] Yaoqiang Xiao, Zhiyi Wang, "Time Frequency Domain Encryption with SLM scheme for Physical Layer security in OFDM-PON system, J.OPT. Communication NETW./VOL..10, NO. 1, 2018.

[19] Xuelin Yang, Xiaonan Hu, ZanweiShen, "Physical Layer Signal Encryption using Digital Chaos in PFDM-PON, IEEE ICICS 2015.

[20] Wei Zhang, Chongfu Zhang, "Brownian Motion Encryption for Physical layer security improvement in CO-OFDM-PON, IEEE Photonics Technology Letters, 2016.

[21] Dana Halabi, Salam Hamdan, "Enhance the security in smart home applications based on IOT-CoAP protocol.

ISBN : 978-93-87793-78-1

[22] Jongsoek Choi, Yongtae Shin, "study on information security sharing system among the industrial IOT service and product provider, IEEE ICOIN, 2018.

[23] Jin HyeongJeon, Ki-Hyung Kim, "Block chain based data security enhanced IOT server platform, IEEE ICOIN, 2018.

[24] MuhammetZekeriyaGunduz, Resul Das, "A comparision of cyber security oriented testbeds for IOT based smart grids, IEEE 2016.

[25] Himanshu Gupta, GarimaVarshney, "A security Framework for IOT devices against wireless threats, second international conference on telecommunication and networks, 2017.

[26] Thomas Maurin, Lurent, George Caraiman, "IOT security assessment through the interfaces P-SCAN test bench platform, 2018 EDAA.

[27] Israr Ahmed, Saleel A.P., BabakBeheshti, "Security in the Internet of things, 4th HCT information technology trends, Dubai, 2017.

[28] Peter Bull, Ron Austin, "Flow based security for IOT devices using an SDN gateway, 4th International conference on future internet of things and clouds, 2016.

[29] IqraHussain, MukeshChandreNegi, "A secure IOT based power plant control using RAS and DES encryption techniques in data link layer", International conference on Infocom technologies and unmanned systems, 2017