IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 5, May 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005126

Lightweight Cryptography and its Algorithms in Internet of Things:An Overview

Parvathy.K

Assistant Professor, Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India

ABSTRACT:An Internet of Things are current emerging technology, where the physical objects are connected in trillion in number. These objects are connected and worked without any human intervention. An IoT is used in many smart applications and due to wide usage in these applications security issues are occurring day-by-day. For keep secure of data in IoT an extreme method are used called lightweight cryptography. These algorithms are mainly working on encryption, hashing and authentication techniques. In this review article, the description on lightweight cryptography are represented. An overview on lightweight cryptography algorithms are mentioned and a few security attacks as well.

KEYWORDS:Internet of Things, Lightweight Cryptography, Symmetric Algorithm, Asymmetric Algorithm.

I. INTRODUCTION

Cryptography[1] is the process of securing the message such as email, card information, etc., The data can be perform the encryption during the transmission on network by using encryption algorithms. In the concept of Network security, the encryption are basic technique used. [3]The encryption are divided into three types they are as Symmetric algorithms, Asymmetric (or public-key) algorithms, and Cryptographic protocols. In encryption and decryption, the algorithms are classified based on size of the keys as symmetric algorithms only single key is used for encryption and decryption. They are also called secret key encryption. Asymmetric algorithms are used two keys as private and public keys. They are also called public key. Public key are used for encryption and private key for decryption. The basic cryptographic algorithms are Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), Triple DES (3DES), Advanced Encryption Standard (AES), RC2, RC6 and Blowfish. Symmetric key encryption are based on the size of key used, as RC2 and DES uses a 64-bit key, Triple DES (3DES) uses two 64- bits keys, AES and RC6 use any of 128, 192 or 256 bits keys and Blowfish uses 32-448 bit range keys (default 128 bits).
AnIoT[3,4,11] is an emerging technology which are used in industry of technology they are used in various industrial applications like vehicles, smart phone TV, Business, Healthcare and fitness have a good features like highly resource-constrained devices where they are having low computational power, memory size is small, power consumption is low, physically small in size and communication is low. [2] Security is most important challenges where limited amount of resource are used. The security goals are been used as confidentiality, data integrity, and authentication in an IoT devices.

II. RELATED WORK

[1]Discusses Cryptographythat is the process of securing the message such as email, card information, etc., The data can be perform the encryption during the transmission on network by using encryption algorithms.[3]illustrates about the concept called the encryption are divided into three types they are as Symmetric algorithms, Asymmetric (or public-key) algorithms, and Cryptographic protocols.The concept about IoT and WSN is discussed using[4,11] is an emerging technology which are used in industry of technology they are used in various industrial applications like vehicles, smart phone TV, Business, Healthcare and fitness.[2]discuss about the Security is most important challenges where limited amount of resource are used.and illustrates about Lightweight cryptography[2] algorithms that need of only low requirements, no criteria are mandatory for this method.[3-11] Discussed about various lightweight algorithms of IoT.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005126

III. LIGHTWEIGHT CRYPTOGRAPHY

Lightweight cryptography[2] algorithms that need of only low requirements, no criteria are mandatory for this method. These algorithms are used in low range of devices in IoT.the features of this algorithm includes consumption power of microprocessor and microcontroller are low. Implementation cost of this method is low. Security is good in the case of performance and cost. During this process, encryption provides the security based on number of rounds.

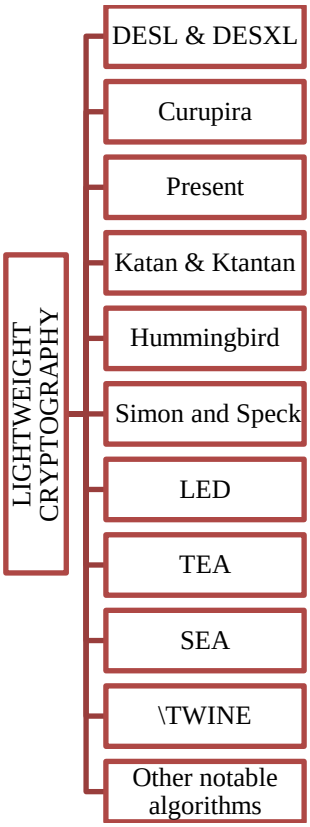

Fig.1.Lightweight Cryptography Algorithms

a)DESL & DESXL

DESL and DESXL[3] is a lightweight versionof algorithms where DESL uses the classical DES algorithm and DESXL uses DESX algorithm. It uses substation block that has a single S-box and it consist of 8 S-boxes. It can resist cryptanalytic attacks by using single S-box and memory.

b) Curupira

Curupira isa[5]Wide Trail strategy-based algorithm invented by Joan Daemen. It has some features which can be helps to perform as lightweight algorithm, the following features as follows:

- data block size = 96 bits Array size as3 X 4-byte array.
- key lengths = 96, 144 or 192 bits;
- number of rounds = based on the key length;
- 8 X 8-bit S-box is implemented as two 4 X 4-bit S-boxes.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005126

C. Katan &Ktantan

KATAN &KTANTAN[6]is a hardware oriented, where it has six block ciphers.They are divided into 3 KATAN ciphers: KATAN32, KATAN48, and KATAN64 and 3 KTANTAN ciphers: KTANTAN32, KTANTAN48 and KTANTAN64.The algorithms are represented as bits based on block size and the number of name in an algorithm. The key size are at 80-bit.

features of Katan &ktantan are as follows as the low resource requirements are

- The size of the internal state is equal to block size of the algorithm. uses shift registers and feedback functions.
- easy to implement in hardware.
- blocks of data which are from 32 to 64 bits;
- key schedule is simple in KTANTAN.

D. Present

the leanest lightweight algorithms[7,8]that has a ISO/IEC standard for lightweight cryptography.The algorithm is based on Serpent and DES by the part of security and hardware efficiency.

The features for this algorithm as follow:

- very less gate count and less memory.
- performs 31 rounds on 64-bit data block
- allows to use 80 or 128-bit keys.
- designed for hardware performance but can be implemented in software.

E. Hummingbird

It is a hybrid algorithm[8] which uses block and stream ciphers. The algorithm work as the encryption as 16-bit blocks of data, uses a 256-bit key, 80-bit internal state and Simple logic and arithmetic operations as uses a small block size. The algorithm performs operations on short 16-bit block size, when compared to PRESENT. it has higher latency and execution time. The algorithm has less encryption speed and is less efficient for authentication mechanisms.

F. Simon and Speck

The lightweight block ciphers[9]designed by the National Security Agency (NSA). this block cipher which was released in June 2013. These block ciphers are used in future applications of IoT.Simon is optimized for hardware implementations. While Speck is optimized for software implementations. The advantages for their work as follows:

- excellent performance on hardware and software platforms
- Very simple constructed
- very easy to find efficient implementations.
- Flexible enough to construct a variety of implementations on a given platform, and
- Open to analysis using existing techniques.

G. LED

LED known to be as Light Encryption Device.[8,9] It is a symmetric block cipher. It is said to be lightweight, that is to be implemented in hardware efficiently. LED is theuse case for the purpose on secure storage and of RFID tags for transmission. It uses a block size of 64 bits. The key length is 64 bit (LED-64) or 128 bit (LED-128). LED can be used for software implementation.

H. TEA

The Tiny Encryption Algorithm (TEA)[10] was designed with the purpose that is to be low and that can perform on small computers. block cipher is based on a high performance. simple encryption algorithmmathematically like Feistel Cipher.

- encrypts 64 bit blocks which are divided into 32 bit blocks.
- Uses a 128-bit length key.
- round based encryption method. The number of the used rounds are variable but 32 Tea cycles.
- It is developed based on the assumption that security can be enhanced by increasing the number of iterations.

The XTEA (eXtended TEA) algorithm is an enhance method of TEA. It works with:

- 64 Bit blocks and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005126

- 128 Bit key length
- 64 encryption rounds.

I. SEA

SEA is known to be Scalable Encryption Algorithm.[10] It has the following features
• Low in memory,
• code size is very Small,
• Limited instruction set.
• Flexibility to run on any platform.

J. TWINE

TWINEis based on a Generalized Feistel Structure (GFS).[8,9] It enables small implementations on hardware and software. It can be implemented in hardware with 1.5 KGates and low-end micro-controllers.it requires several iterations to make the resulting cipher sufficiently secure. TWINE employs an improved variant of GFS which results in making it to be ultra-lightweight while keeping sufficient speedto recover this drawback. TWINE is Type-2 generalized Feistel [20] with following features:

- 64 bits block size
- 36 rounds
- TWINE has two types - TWINE-80 and TWINE-128 where the key size is 80 bits and 128 bits respectively.

K. Other Algorithms

Other notable algorithms are listed below:

- **Skipjack**[7]is a lightweight block cipher based on an unbalanced Feistel network for embedded applications. It operates on 64-bit block length with 80-bit key.

- **NOEKEON[8]** is a hardware-efficient block cipher.

- **HIGHT[9]** was a generalized Feistel-like cipher as it possesses 64-bit block length and 128- bit key length to be suitable for low cost, low-power, and ultralight implementation.
- **Crypton[9]** bis a compact implementation of which is used in both hardware and software.
- **KeeLoq[10]** is a lightweight block cipher with a 32-bit block size and a 64-bit key. Despite its short key size, it is widely used in remote key less entry systems and wireless authentication applications.

IV. CONCLUSION

An Internet of things which consist of physical objects that are connected with the networks. The physical objects that perform communication among each other. The security is one of the important challenges during the communication in IoT devices. For securing of data cryptography is used. In this paper lightweight cryptography and its algorithms are introduced by explaining the overview on lightweight cryptography and its types of the algorithms that are used in an Internet of Things devices.

REFERENCES

[1] W. Stallings, Cryptography and Network Security, Prentice Hall, pp. 58-309, 4th Ed, 2005.
[2] Paar, Christof, Pelzl, Jan; Understanding Cryptography, A Textbook for Students and Practitioners; First Edition, 2010. ISBN 978-3-642-04100-6 e-ISBN 978-3-642-04101- 3 DOI 10.1007/978-3-642-04101-3.
[3] Studying the Effects of Most Common Encryption Algorithms, Diaa Salama, Hatem Abdual Kader, and MohiyHadhoudJazan University, Kingdom of Saudi Arabia Minufiya University, Egypt, International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.
[4] Evaluating the Performance of Symmetric Encryption Algorithms, Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2, International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 5, May 2021||

DOI:10.15680/IJIRSET.2021.1005126

[5] Idrus.S.Z, Aljunid.S.A, Asi.S.M (2008), "Performance Analysis of Encryption Algorithms Text Length Size on WebBrowsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, PP 20-25.

[6] Christophe De Canni`ere and Orr Dunkelman, Miroslav Kneßzevi´c, "KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers".

[7]SushaSurendran (NYIT, Abu Dhabi, UAE), Amira Nassef (NYIT, Abu Dhabi, UAE), Babak D. Beheshti (NYIT, Old Westbury, New York), A Survey of Cryptographic Algorithms for IoT Devices,IEEE.

[8] Hamid Bostani , Mansour Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach ", 0140-3664/© 2016, Elsevier.

[9] Ms. Snehal Deshmukh, Dr. S. S. Sonavane, "Security Protocols for Internet of Things: A Survey", ICNETS2, VIT University, Chennai, 2017, 978-1-5090-5913-3/17/$31.00_c 2017 IEEE.

[10] Amrita Ghosal, Subir Halder, "A survey on energy efficient intrusion detection in wireless sensor networks", Journal of Ambient Intelligence and Smart Environments 9 (2017) 239–261, DOI 10.3233/AIS-170426.

[11] Kamaljit Kaur, Ramanjot Kaur, "A Literature Survey on Security & Privacy Issues in IoT," *International Journal of Computer Sciences and Engineering*, Vol.9, Issue.4, pp.60-64, 2021.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details