International Journal of Engineering & Technology, 7 (2.7) (2018) 887-890

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A Study on Light Weight Cryptography Algorithms for Data Security in IOT

M. Sri Lakshmi [1]*, V. Srikanth [2]

[1,2]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India – 522502
**manchala.srilakshmi@kluniversity.in*

Abstract

IOT - things like the smart devices and sensors that connects and communicates through Internet. IOT applications like smart home, smart vehicles, smart retail, which makes the mankind's life easier. There is a prediction that we will be having million of devices connects to the Internet. Since the sensitive devices like baby monitoring devices, health monitoring devices are the part of interconnected world there is the necessity to address the consequence of the security aspects of the IOT. The built-in nature of the IOT is to trace user's identity easily, so the security and privacy concerns like stealing the data, disruption of operations and even the loss of life are becoming critical issues in today's IOT applications. Due to the resource constrained environment in IOT the conventional algorithms is not enough to ensure the data security. So we need a less computational cost in terms of power consumption and memory management and more efficient cryptography algorithms which are discussed in this paper.

Keywords: *Attacks; Internet of things; Light weight cryptography algorithm; Security and Privacy.*

1. Introduction

The era of internet has been changed to connecting million smart devices that connects anything anywhere and anytime I.e. internet of things[1]. The number of interconnected devices are more than the number of human beings which are expected to be increased by 2020. In IOT the data is collected from various sensors, smart devices that are connected in the network, so that the users can access the data. IOT played a eminent role in the day to day life's of humans in several ways. Some of the applications[2] of IOT are:

Home Automation System: The users can control the electronic gadgets like AC, Fan, lights, through their mobiles which helps in reducing the energy consumption. IOT is used to develop the security systems for their homes which can reduce the risk of the threats and thief.

Transport Systems: The users can prevent the accidents by gaining the knowledge of the obstacles which comes in front of them by using sensors, can report the accidents to the authorities, and can monitor the traffic-jams.

Health monitoring devices: which helps in monitoring the remote patients, assisting the old age people and these days the baby monitoring devices are even under developing.

Surveillance: which is used to track the people, animals and objects.

1.1. IOT Architecture

In IOT not only the sharing of information happens but the decision making as well happens. This can be explained **the** basic IOT Architecture[3] which is divided in to three layers.

1. Perception layer: This layer helps in collecting the information from various devices like sensors, actuators, RFID tags.

2. Network layer: The layer responsible for the transmission of the data from the perception layer to the user is the network layer. This layer is used as information center.

3. Application Layer: This layer is the bridge between the technology and the human needs.

1.2. Research Motivation

Recent studies shows that the kind of openness and less human intervention in IOT, it is exposed to several attacks like DDoS attack, man-in-the-middle attack, warm hole attacks. Attacker can gain the access to the network can damage the physical devices of IOT can damage the network which compromises the privacy and security of IOT. As the IOT devices have low memory, less power and bandwidth an efficient solution to provide security is needed that will not chomp through the resources of IoT. The prime objective of this research paper is to provide an overview of to show the need for light weight cryptography algorithms and the analysis of the existing algorithms which are vulnerable to several attacks.

1.3. Overview of the Security attacks in IOT

As the communication happens through internet in IOT, there is more possibility of the attacks happens as the internet is public networks. The security attacks are divided **into** four categories, Physical, network, software and encryption attacks. Security aspects of IOT are in terms of privacy, technological and ethical. A massive DDOS (Distributed Denial of Service) attack has occurred in 2016 on DYN company which controls the Internet by a botnet which induced a malware that gained access to the

large number of IOT devices which shows the need for more research work in security domain of IOT. In this section a review of various security issues in each layer of IOT architecture is discussed.

Perception Layer

The perception layer[4] is designed for collecting the data from the physical devices like RFIDs, sensors (temperature, pressure, gas, etc) and actuators which are termed as nodes that is responsible for data control and data acquisition. There is need to detect the abnormal or the faulty nodes which happens when the node is attacked physically or compromised by cyber attacks. In order to avoid the in-efficiency of the service: Chen proposed a localized faulty detection algorithm to identify the faculty nodes. Da silva proposed decentralized intrusion detection system. IEEE 802.15.4 security solution is also available.

Network layer

The responsibility of the network layer is to transfer the data securely to upper layers which was gathered at the perception layer. The security attacks that happen in the network layer is man-in-the-middle attack, Distributed DoS attacks, unauthorized access of the network, eavesdropping, wormhole attack, damage of confidentiality and integrity, insertion of the malware. Disclosure of user's privacy is the main concern in the network layer.

Application Layer

IOT has many applications like smart home where electronic gadgets are controlled by the mobile app and smart cities with smart parking and smart street lights, smart environment, smart industries etc. as these applications are at the computer level hacking of the system is possible and that could get infected with virus and Trojans. Leakage of the data and user's privacy is one of the most common issue that occur in the application layer.

1.4. Cryptographic algorithms in IOT

The limitations of the IOT devices are energy consumption and computational power. Execution of strong security instruction uses lots of device power, which is not recommended all the time due to the IOT devices which are designed to be small where the batter life cannot be extended. So the conventional cryptography algorithms which require high energy and memory consumption is not enough for the present IOT applications to ensure data security and authentication. A light weight cryptography is combination of light weight in terms of software and hardware requirements of the applications and security. Software requirements of the algorithm are in terms of processing speed and time complexity. The hardware requirements of the algorithm are memory and battery life. The light weight cryptography algorithms are designed by using the block cipher algorithms where the performance will be better when compared to stream ciphers.

The Prime Objectives of the light weight Cryptography Algorithms are the structures used in the algorithms, the smaller key sizes and small block length and the number of rounds which reduces the computational cost so that the energy consumption of the devices can be reduced. The main concern that has to keep in mind while developing the light weight cryptography algorithm is the key size and length of the block. If the size of the key is increased then the computation cost and the number of rounds to perform the encryption and decryption is increases which consumes more energy of the device. A multi-key attack is the most common issue that happens when the attackers tries to break the encryption under one particular key. So the confidentiality will be compromised as the attackers will be successful in gaining the initial key.

Performance metrics of low resource devices for light weight cryptography:

The performance of a light weight cryptography is latency, energy consumption through put and wait time. In order to achieve these metrics we have two ways:
Software implementation: it is nothing but the running of cryptographic code on processor. The software implementation for a low resource constraint devices is in-terms of power consumed, memory occupied, and processing speed. The specific software metrics is the number of registers required in ROM and RAM.
Hardware implementation: The main requirement for the hardware implementation in IOT is the platform where the algorithm is implemented. We have hardware platforms like FPGA, ASIC etc. which minimizes the developing cost and increase the flexibility. The design time is reduced in ASIC due to automated design flow.

Light Weight Ciphers
Cryptography is the way to ensure the data security by encryption the process of converting the plain text into cipher text and decryption – the process of converting the cipher text into plain text. But the problem with this process is breaking of the encryption algorithms by series of attacks. The algorithms with more number of rounds and larger key size can be used to achieve the data security. But in IOT where the devices are designed to be small with less resources the existing algorithms like DES, RSA, RC5 etc can be used to high computational power. Hence there is necessity to go for the light weight cryptography algorithms.

2. Literature survey of Cryptographic algorithms

Cryptography algorithms are of two types: Symmetric and Asymmetric. Symmetric algorithms use a single for both encryption and decryption. Confidentiality and Integrity of the data is achieved using symmetric algorithms. But the Authentication is not achieved. The disadvantage of this algorithm is distribution of the key between the sender and the receiver as they both use the same key for communication. Conventional Symmetric Algorithms are DES, AES, Triple DES, IDEA, Blowfish[5] which can not be used to for IOT devices due to their larger key sizes, larger block lengths and vulnerable to several attacks like brute force attacks.
Asymmetric Algorithms uses two key public and private keys in communication. Confidentiality, Authentication and Integrity is assured by Asymmetric algorithms. In order to achieve integrity and confidentiality the sender encrypts the data by using receiver's public key and the data can be decrypted only by the receivers private key.
To achieve the authentication the sender encrypts the message by his own private key and the data is decrypted by the sender's public key at the receiver side[6]. The commonly used asymmetric algorithms are RSA, ECC(Eliptical curve cryptography and Deffie Helmen key exchange and Hash Functions. The limitation of this algorithms is larger key size which increases the complexity of the algorithm and increases the computational cost which again is not feasible for the IOT devices which can not afford for more computational power and energy consumption. So light weight cryptography algorithms are proposed which are described below.

HIGHT(High Security and Light weight):

HIGHT is built on the Feistel Structure. It has 64 bit block size, 128 bits key size and 32 rounds of encryption and decryption are performed[7,8]. The basic operations of the HIGHT algorithms are Addition, mod, XOR. This Algorithm require less power con-

sumption and good for RFID tagging. It is vulnerable to differential and saturation attacks.

AES (Advance Encryption Standard): This algorithms is based on substitution permutation network. It has block length of 128 bits. The key sizes are 128,192 and 256 bits. The operations are used in this algorithm are AddRoundkey, subbytes, shiftrows and Mixcolumns[9,10]. Even though we are using the different key sizes the algorithm is still prone to man-in-the-middle attack, related key attack**.**

PRESENT: This algorithm is also based on substitution permutation network structure. It is an ultra light weight algorithm for data security in IOT[11]. It has block length of 64 bits with key size of 80 or 128 bits and 32 rounds of operations are performed in this algorithm. It uses S-boxes for operations Differential attacks, side channel attacks happens on this algorithm.

RECTANGLE: This algorithm[12] is based on substitution permutation network structure. It is a ultra weight bit-slice block cipher which works efficient for multiple platforms that has less area in hardware and shows good performance in software implementations when compared to other algorithms. It supports 80 or 128 bits key size , 64 bits block length with 25 rounds of operations.

CLEFIA: This algorithm is built on Feistel network that was standardized in 2007 by NIST[13,14]. This is other type of light weight algorithm which showed good performance in security. It has key size of 128, 192 and 256 bits and block length of 128 bits. It showed greater performance in hardware implementation of cipher when compared to other ciphers. This algorithm is vulnerable to saturation crypt analysis.

CAMMELLA: This algorithm is the symmetric block cipher that has a block length of 128 bits and key size of 128,192 and 256 bits. This algorithm[15,16] showed better efficiency in both software implementations and hardware implementations when compared to other ciphers. It is used for network with high speeds and low smart cards.

TWINE: The key size of this algorithm is 80 and 128 bits. It has block length of 64 bits with 36 rounds[17,18]. Every round operation contains a non linear substitution layer using 4- bits S-boxes and a diffusion layer which permutes the blocks (4 bits). Its is based on the Feistel Network structure. It works efficiently for small hardware environments. The most common attack that happens on the algorithm is the man-in-the-middle attack.

SPECK algorithm is designed for the software implementations where as SIMON is designed for hardware implementations. The below table shows the different light weight algorithms compared in terms of block length, key size and rounds, performance metrics ,attacks and merits[19].

Table 1: Summary of light weight cryptography Algorithms

S.No	Algorithm	Performance		Attacks	Merits
		Power (µW)	Throughput At 100Khz(kbps)		
1	CLEFIA	2.48	39	Saturation Cryptanalysis	Energy Efficient due to less no. of rounds in cryptography
2	CAMELLIA	1.54	290.1	Cache timing attacks	Resistance to Brute Force attack on keys
3	SPECK	1.40	12.1	Key recovery, Boomerang attack	Performance better in software
4	HIGHT	5.48	188.20	Impossible differential attack	Provides high security, good for RFID tagging
5	RECTANGLE	1.78	246	Slide attack, statistical, Saturation Attack	Fast implementations using bit slice techniques
6	PRESENT	1.54	12.4	Internal, Bottleneck attacks, side channel attacks	Ultra Light Weight, Energy cipher, Energy efficient
7	AES	2.481	56.64	Related key attack, Boomerang, Biclique, cryptanalysis	Supports larger key sizes, faster in both hardware and software
8	TWINE	1.30	178	Saturation attack, Meet-in-the-middle attacks	Efficient software implementation and Good for small hardware
9	SIMON	1.32	22.9	Differential fault attacks, Attacks on reduced versions	Supports several key sizes, performs well in Hardware

The table above shows that the algorithms build using Feistel Structures showed better performance when compared to others as it uses same hardware for encryption and decryption to reduce execution time and memory. If the algorithm has the more number of rounds for both encryption and decryption degrades the performances. So in future the hybrid models should be developed to reduce the computation power and increase the efficiency of data security in IOT applications[20]when compared to the conventional algorithms.

3. Conclusion

In future IOT becomes the most essential part of the mankind for quality life. Large amount of sensitive data is communicated between the devices with resource constraints like less memory space, low power where the data security is the main concern. The conventional algorithms which requires more computational power and memory which is not good enough for the present scenario with IOT. Hence light weight cryptography algorithms are need. This paper provides an overview of the light weight cryptography algorithms for data security which are still vulnerable to different kinds of software and hardware attacks in IOT . It is essential to develop a more secured light weight cryptography algorithms that has low computational cost, more processing speed and smaller key size.

References

[1] K. Zhao and L. Ge, “A Survey on the Internet of Things Security,” in Ninth International Conference, on Computational Intelligence and Security, Dec. 2013, pp. 663-667.

[2] R. Khan et al., “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” in 10th Interna-

tional Conference on Frontiers of Information Technology, Dec. 2012, pp. 257-260.
[3] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," in Computer Communications, 54, pp.1-31.
[4] M. Wu et al., "Research on the architecture of Internet of Things," in 3rd International Conference on Advanced Computer Theory and Engineering, 2010, pp. 484-487.
[5] K. Acharya et al., "Analysis of Cryptographic Algorithms for Net work Security," in International Journal of Computer Applications Technology and Research, 2013, Vol. 3, No.2, pp. 130-135.
[6] T. Eisenbarth et al., "A Survey of Lightweight-Cryptography Implementations," in IEEE Design & Test of Computers, 2007, Vol. 24, No.6, pp. 522-533.
[7] H. Yap et al., "EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption," in Cryptology and Network Security Lecture Notes in Computer Science, Springer, 2011, pp. 76-97
[8] D. Hong et al., "HIGHT: A New Block Cipher Suitable for Low-Resource Device," in Cryptographic Hardware and Embedded Systems - CHES 2006 Lecture Notes in Computer Science, 2006, pp. 46-59
[9] A. Moradi et al., "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," in Advances in Cryptology – EUROCRYPT 2011 Lecture Notes in Computer Science, Springer, 2011, Vol. 6632, pp. 69-88
[10] M Feldhofer et al., "Strong Authentication for RFID Systems Using the AES Algorithm," in Cryptographic Hardware and Embedded Systems – CHESS 2004 Lecture Notes in Computer Science, Springer, 2004, pp. 357-370.
[11] Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, Vol 4727. Springer, Berlin, Heidelberg
[12] W. Zhang et al., "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," in Science China Information Sciences, 2015, vol. 58(12), pp. 1-15.
[13] T. Akishita and H. Hiwatari, "Very Compact Hardware Implementations of the Blockcipher CLEFIA," in Selected Areas in Cryptography Lecture Notes in Computer Science,Springer, 2012, pp. 278-292.
[14] T. Shirai et al., "The 128-Bit Blockcipher CLEFIA (Extended Abstract,)" in Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, Springer, 2007, Vol.4593.
[15] Isha and A. K. Luhach, "Analysis of Lightweight Cryptographic Solutions for Internet of Things," in Indian Journal of Science and Technology, 2016, Vol. 9, pp. 28.
[16] A. Satoh and S. Morioka, "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," in Lecture Notes in Computer Science Information Security, Springer, 2003, pp. 252-266
[17] T. Suzaki et al., "TWINE: A Lightweight Block Cipher for Multiple Platforms," in Selected Areas in Cryptography Lecture Notes in Computer Science, Springer, 2013, Vol. 7707, pp. 339-354.
[18] P. Kumarkushwaha et al., "A Survey on Lightweight Block Ciphers," in International Journal of Computer Applications, 2014, vol. 96(17), pp. 1-7.
[19] R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers," in Proceedings of the 52nd Annual Design Automation Conference, 2015, pp. 1-6
[20] Isha Bhardwaj,Ajay Kumar,Manu Bansal, "A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs" in Proceedings of the 4th International Conference on "Signal Processing, Computing and Control" Sep 2017.