Real Time Key Authentication in IoT

Project Report submitted in partial fulfillment of the requirement
for the degree of

Master of Technology

in

Computer Science & Engineering

Under the Supervision of

Dr. Hemraj Saini

By

Effy Raja Naru, Roll No. 152212

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

Certificate

This is to certify that Project report entitled **"REAL TIME KEY AUTHENTICATION IN IoT",** submitted by **Effy Raja Naru** in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat Solan has been made under my supervision.

This report has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date:1th May.2017

Dr. Hemraj Saini

Associate Professor

Department of Computer Science & Engineering,

JUIT, Solan H.P.

Acknowledgement

First and foremost, I would like to express my deep sense of gratitude to my supervisor **Dr.Hemraj Saini** for providing the excellent guidance during my research and study at Jaypee University of Information Technology,waknaghat,Solan(H.P). The door to Associate Prof. Saini office was always open whenever I ran into a trouble spot or had a question about my research.

My frequent interactions with him in all aspects of the report writing have been a great learning experience for me. I shall always cherish his support and encouragement.

I would like to express my profound sense of gratitude to all faculty members for their valuable suggestion especially **Miss. Geetanjali.**

Finally, I must express my very profound gratitude to my parents and to my sister proving me with unfailing support and continuous encouragement throughout my years of study and this accomplishment would not have been possible without them. Thank you.

Date: 1th May.2017

Effy Raja NARU
152205

Table of Contents

Certificate………………………………………………………………………..i

Acknowledgement……………………………………………………….....ii

List of contents………………………………………………………….iii

List of abbreviations……………………………………………………….v

List of Figures……………………………………………………………..vi

List of Table…………………………………………………………………vii

Abstract……………………………………………………………….…..viii

Chapter 1: Introduction

1.1 IoT 1

1.2 IoT Architecture 2

1.2Problem Statement 3

1.3 Objectives 3

1.4 Outline 3

Chapter 2: IoT Overview

2.1 IoT applications 5

2.2 IoT Security Attack 6

2.3 lightweight Cryptography 8

2.4 Summary 19

Chapter 3: Hardware Equipment

3.1 Raspberry Pi 21

3.2 Arduino Duemilanove 23

3.3 Xbee module 23
3.4 Summary 24
Chapter 4: LITERATURE REVIEW
4.1 Literature 25
4.2 Summary 30
Chapter 5: Proposed Solution
5.1 Proposed IoT Security architecture 31
5.2 Proposed Approach 33
5.3 Summary 39
Chapter 6: Implementation and Result Analysis
6.1 Result Analysis 41
6.2 Summary 44
Chapter 7: Conclusion and Future Work
7.1 Conclusion 46
7.2 Future Scopes 46
References 47

Abbreviation and Symbols

IoT	Internet of thing
RFID	Radio-frequency identification
HEDUN	Hybrid encryption and decryption
4G	4th Generations
3G	3rd generations
CIA	Confidentiality Integrity Availability
AES	Advanced Encryption Standard
ECC	Elliptical curve cryptography
IBE	Identity-Based Encryption
CP-ABE	Cipher Policy Attribute-Based Encryption
KP-ABE	Key-Policy Attribute-Based Encryption

List of Figures

Title	Page No.
Figure 1.1 IoT Elements	1
Figure 1.2 IoT Architecture	2
Figure3.1 Thesis Outline	4
Figure 2.1 IoT applications	5
Figure 2.2 IoT Security Attacks	6
Figure 2.3 Internet security Threat	7
Figure 2.4 key size growth	9
Figure 2.5 Lightweight cryptography used in IoT	10
Figure 2.6 Symmetric key	11
Figure 2.7 Present Block Cipher	11
Figure 2.8 IDEA Block	12
Figure 2.9 four key transformations	13
Figure 2.10 Asymmetric PKI	14
Figure 2.11 Types of Attribute-Based encryption and decryption	15
Figure 2.12 KP-ABE Process	16
Figure 2.13 CP-ABE	17

Figure 2.14 AAβ Encryption 18

Figure 2.15 AAβ Decryption 18

Figure 2.16 Advantage of signcryption 19

Figure 3.1 Types of hardware equipment 21

Figure 3.2 Raspberry Pi 22

Figure 5.1 Proposed IoT Security Architecture 31

Figure 5.2 Notarization Architecture 32

Figure 5.3 Proposed Approached 33

Figure 5.4 Considered parameter in a proposed approached 35

Figure 5.5 Flow diagram 36

Figure 5.6 Proposed Technique Phase 36

Figure 5.7 Encryption steps 37

Figure 5.7 Decryption steps 38

Figure 5.8 digital signature process step 39

Figure 6.1 Block diagram of our Implementation proposed technique 41

Figure 6.2 Proposed HEDUN time using notarization 42

Figure 6.3 time difference of RSA using notarization 43

Fig ure 6.4 Time difference of RSA using notarization 44

List of Table

Title	Page No.
Table 1 The operating system requirement	2
Table 2 Requirement	8
Table 3 key size recommended by NIST	9
Table 4 Present block cipher key and round	11
Table 5 Block and key size of IDEA	12
Table 6 block size and the key size of blowfish	12
Table 7 The AES 128 bit Parameters	13
Table 8 Characteristic Raspberry Pi	22
Table 9 Characteristic of Arduino Duemilanov	23
Table 10 Characteristic of xBee pro	23
Table 11 Comparisons Between Related Works	29
Table 12 Compressive study with Parameter	34
Table 13 Encryption and decryption time of HEDUN	41
Table 14 RSA using notarization encryption and decryption time	42
Table 15 IBE using notarization encryption and decryption time	.43
Table 16 Comparison table of existing and proposed approaches	43

Abstract

The Internet of Things (IoT) is the future of the next era of the internet which connects various physical objects that communicate with each other without the aid of human interactions and used current internet standards protocol for sharing the information over a public network. Lightweight cryptography is recently filed in the cryptography that is custom fitted resource constrained devices in IoT. Lightweight cryptography implies that are implemented in resource-constrained environments in IoT for encrypting and decrypting the data. Lightweight Asymmetric cryptography is more secure than Lightweight symmetric cryptography in light of some lightweight symmetric block cipher is split like TEA and so forth. Design intelligent gateway with notarization security system for execution encryption and decryption strategies in term of software implementation for class-0 devices. In this arrangement intelligent gateway which endow data aggregation and filtering of data. Notarization security component set up the trust third party for generating the public and private key for encryption and decryption for class-0 devices. The Notarization strategy is utilizing java micro edition software development kit that gives the adaptable condition to an application running on resource-constrained devices in IoT.

CHAPTER 1

INTRODUCTION

Chapter one is partitioned into two sections. The first sections describe the IoT element and the IoT architecture. Second sections explain problem statement objective and layout of the thesis.

1.1Internet of Things

The Internet of Things (IoT) [1] is the future of the next era of the internet which connects various physical objects that communicate with each other without the aid of human interactions and used current internet standards protocol for sharing the information over a public network. Internet of Things is the combinations of three terms (i) Things pinpoint itself (ii) Thing commutations (iii) Thing interact that builds the Ubiquitous computing [2] environment. IoT element is divided into six parts these six elements is needed for the functionality of IoT Fig.1.1 has shown IoT element identification most important element of IoT to identify the object-id and address in IoT environment. IPv6[7] and IPv4 address method used for addressing in IoT. The sensing element is gathering the data from related objects. Sensors and actuators are used by sensing element. Communication element used for transmitted the information gathered and collected by sensing element. Wi-Fi, Bluetooth, element example of communication element. The computation element is the brain of the IoT. All Processing of IoT is done by computation element (e.g., microcontrollers, microprocessors, operating systems etc).IoT services element define the services provided by IoT(e.g., smart home, smart parking system etc).Semantic element provided the required services (e.g., Semantic Web, Efficient XML Interchange etc).

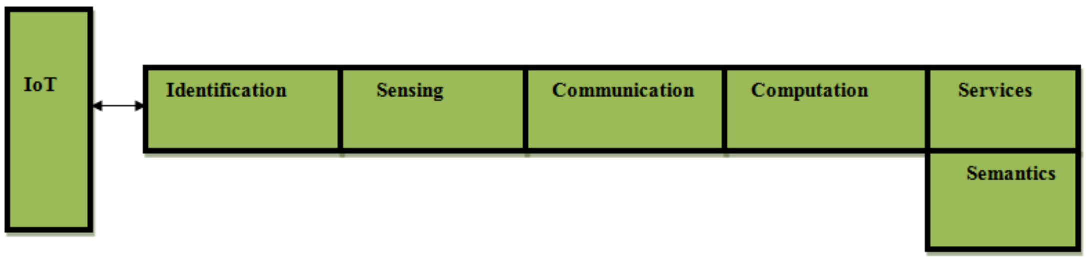

Fig. 1.1 IoT Elements

Operating system design for IoT is most of supporting the real-time system in Table 2 show the operating system comparison in terms of memory, language support, multithreading, IPv6 support and real time Used in IoT. Where P means partially in the Table 1.

OPERTING SYSTEMS	MINIMUM MEMORY	LANGUAGE SUPPORT	MULTITHREADING	REAL TIME	IPv6 support
LINUX	1MB	C,C++	YES	P	YES
RIOT	1.5 KB	C,C++	YES	YES	YES
CONTIKI	2KB	C	YES	P	YES
ANDROID	--	JAVA	YES	P	YES
TINYOS	1KB	Nes c	PARTIALLY	NO	NO

Table 1 Operating system requirement

1.2 IoT Architecture

Usually, IoT designs are isolated into three-layer models (i) physical layer (ii) commutation layer and application layer. The primary layer is physical layer (is also called perceptual layer) is in charge of gathering data for each object and consist of constrained devices/unconstrained devices.

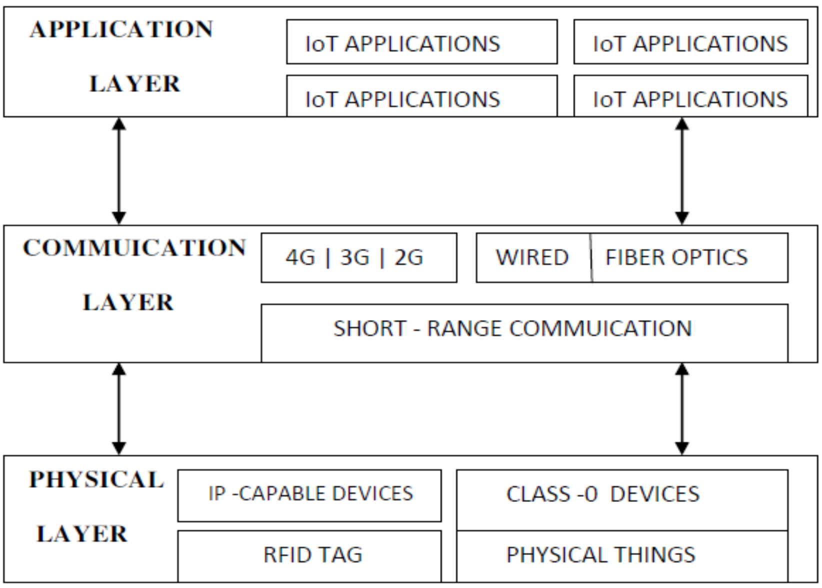

Fig. 1.2 IoT Architecture

The second layer is communication layer that is responsible for transmitting the data gathering from the physical layer. While the transmission media, as 4G,3G,2G, wireless, wired, fiber-optic, short range communications for commutating the data over a public network. The third layer is the application layer capable of recognizing the mold of application which will be used in IoT. Fig. 1.2 has shown IoT architecture .

Problem Statement

Traditional network-centric devices, for example, firewalls can't be ensured information In the IoT environment .Devices that are connected in IoT are resource constrained. IoT end nodes to directly usage an encryptions and decryption technique in term of software is difficult due to their obliged in memory and computational power particularly in class-0 devices, class-0 devices support maximum RAM 10 kb and 100 kb ROM. So some asymmetric encryption and decryption strategy may not relevant due to their resource intensive because they key size is large and required complex operation. A surrogate software implementations mechanism for securing date transmission certainly in these devices required.

Objective

In this research the following objective indentify as fellow:

- Study various lightweight encryption and decryption technique that are secure and take a less time for encryption and decryption process.
- Identify standardizes encryption and decryption technique that are recommended by NIST for resource constrained devices.
- Design the notarization mechanism for generating encryption and decryption key using standardizes encryption and decryption technique in less time as compare to RSA.
- Propose hybrid encryption and decryption technique that generating the key and key administration by notarization for secure the data in IoT.
- Evaluate and analyze the time take by the propose technique for encryption and decryption process.

Thesis Outline

Chapter two describes the IoT application, security attack and lightweight cryptography. Chapter 3 explains the existing literature review related to IoT lightweight encryption and decryption techniques. Chapters four discuss the proposed solution and proposed technique for encryption and decryption process. Chapter 5 discusses implementation and result analysis and compressive study. Finally chapter six explains the conclusion and future work. Figure 1.3 depicts the thesis outline.

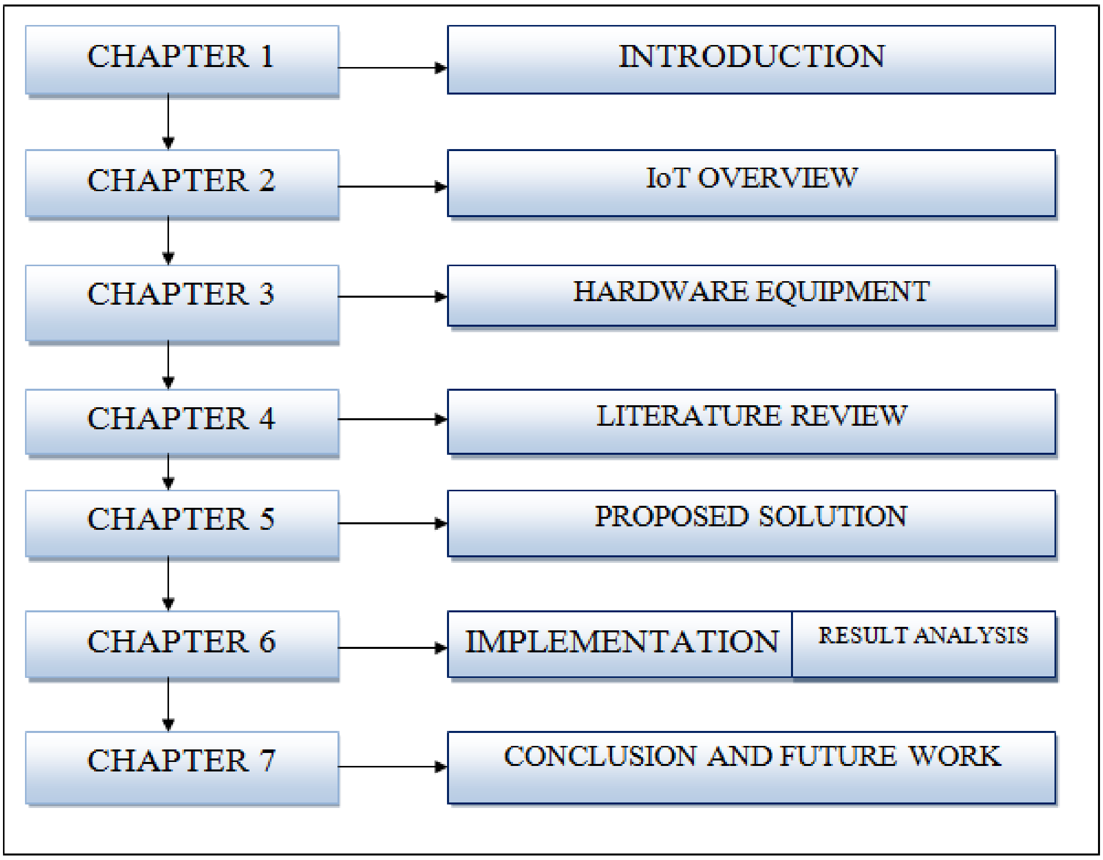

Fig. 1.3 Thesis Outline

CHAPTER 2

Overview IoT

Chapter two is partitioned into four sections. The first sections describe the IoT application. Second sections explain security attack on IoT. Third sections describe the lightweight cryptography and last section summarization of the chapter.

2.1 IoT APPLICATIONS

IoT plays important role in day to day lifestyle. Various IoT applications improve the lifestyle of human in the earth. Figure 2.1 has shown some IoT applications.

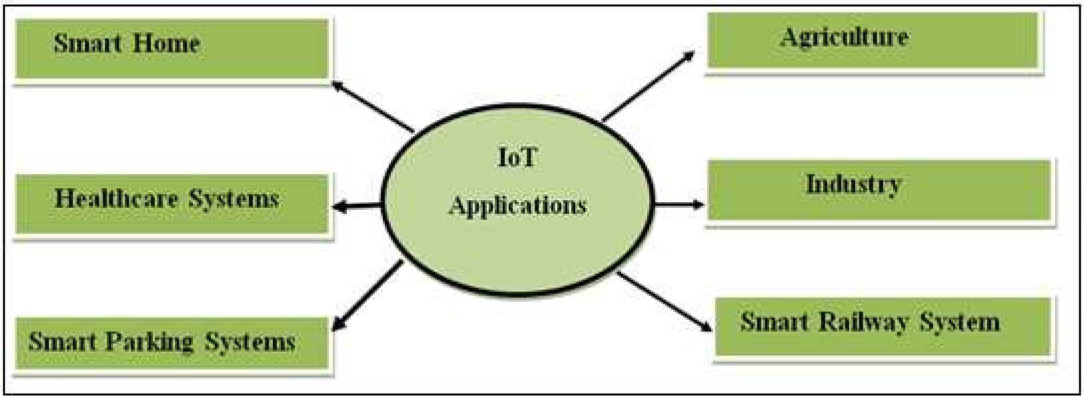

Fig.2.1 IoT applications

smart home[6] application of IoT information is gathered by different IoT sensors and actuators and information exchange to controls unit that naturally controls the capacity of brilliant home like a light on or off and monitoring. Smart home improves the inhabitant quality of the life. Everyday lot of people dies because they don’t get timely medical help. IoT is played an impotent role in healthcare system [8] to give opportune therapeutic treatment utilizing different body sensors (e.g., EEG sensors, ECG sensors) and furthermore supportive for older people and physical disability. The smart railway system is a vital application of IoT. According to a high-level safety review committee around 15000 people killed every year in the railway accident in India. Different IoT sensors such (temperature sensors, fire sensors, fault sensors track observing sensors) used to make an intelligent railway system. to stop these accidents and monitoring the railway stations. In goods industry IoT improve the processing time of the products etc. IoT is also suitable for agriculture various IoT sensors (temperature sensors, rainfall sensors) provided the information for farmers related to rainfall, temperature etc. IoT is changing the traditional agriculture style to intelligent agriculture style.

2.2 IoT SECURITY ATTACK

In the conventional network, security attack is an action that destroys, modify, screen the data and enable the unapproved individual to get to the access of the system. Like an ordinary network, IoT is enduring from different security assaults. IoT assault isolated into five types as the fellow

(1) Physical attack

(2) Passive attack

(3) Active attack

(4) Attack on cryptography

(5) Routing attack.

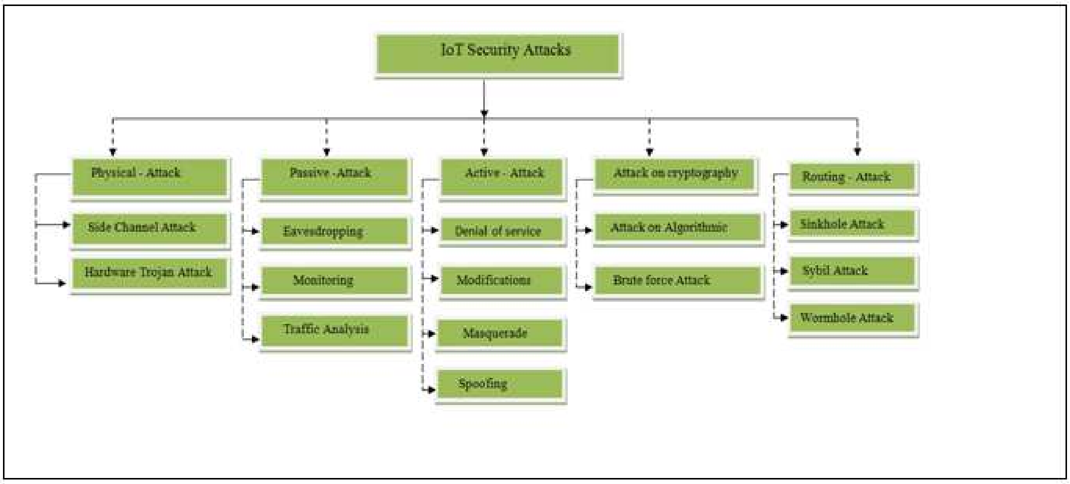

Fig. 2.2 IoT Security Attacks

"In Physical assaults, attackers principally concentrate on devices. Well known class of physical assault is side channel Attack[3].Side channel assault is a capable assault to recapture the secret key from the devices. Side channel assault utilizing side channel data (e.g, EMF, timing data, control usage, discharge and so on) and the inside outline of handling devices to recapture the secret key from the devices. Side channel assault is a non-invasive physical attack.In non-invasive attack assailant set up the assaulting environment utilizing pieces of equipment such as the aging antenna, oscilloscopes, function generators etc.The thought behind side channel assault is watching the side channel information of devices. The another physical assault is hardware trojan attack[9].Hardware trojan assault is like software trojan attack.A

Hardware trojan assault is by a pernicious change in the integrated circuit during design and manufacture utilizing untrusted people.

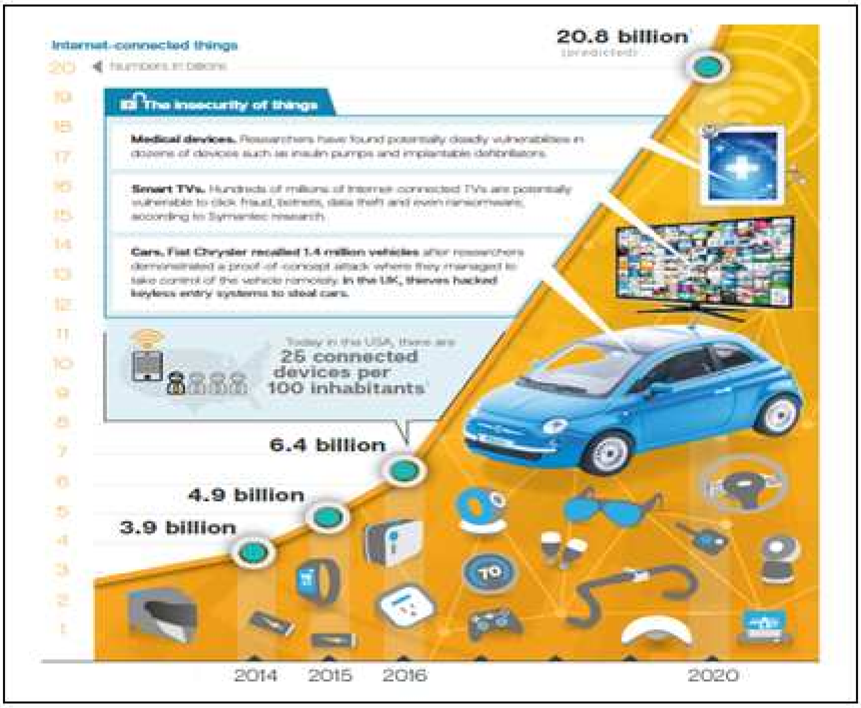

Fig. 2.3 Symantec Internet Security Threat Report [14].Source: Symantec

Like conventional passive attack and active attack, IoT is an also endured from the passive an active attack. A passive assault does not influence the system resource in this type of assault alteration of information is not the purpose of attackers.In this assault Attackers chiefly to pick up the data of the target.An eavesdropping is communication layer assault in which capture the information transmitted over the public network. Monitoring attack is also communication layer attack in which attacker read the information but does not change the information.In traffic analysis assault aggressor examination how much information move in a correspondence way amongst sender and receiver. A active assault affects the system resource this kind of assault alterations of information is the principle objective of the attackers. Denial of services assault is the Most powerful active attack in communication layer at IoT. Denial of services assault is the type of assault where attackers try to attempt to send the bulk of data to the server to the prevent legitimate user to accessing the services.is the types of denial of services attack on distributing network in IoT to prevent legitimate user to user to accessing the services.In this type of assault malicious node sending the message to the server and expending the data transfer capacity of the channel and make the server asset inaccessible to clients. Botnet [10] is the number of computer devices associated with internet and control by the one botnet master to perform out a different assault (DDOS) on IoT. Modification assault malicious node change the message send by a sender or alter the route of the sender that causes the long communication delay. In masquerade assault assailant has utilized the identity of a legal user to stealing user credentials. Assaults on cryptography assailant primarily concentrate on the algorithms in this type of assault intruder find the weakness of the algorithms and attempt to crack algorithms logic. The other cryptography assault is brute force assault depends on hit and trial technique to break the secret key and password of the legitimate users. Routing assault is characterized as the assault that is performed on the routing table, routing protocol and changes the routing route. Sinkhole assault [11] is the assault in which malicious nodes pull in information encompassing node in its neighboring node and report its fake routing update. Sybil attack [12] attackers can manipulate multiple copies of malicious nodes. Wormhole attack [13] is tunneling attack in which attack intruder capture the packet from one point at network and tunnel to the malicious nodes in the network. Every year an expanding number of different security assaults on IoT brought up by the Symantec Internet Security Threat Report Figure 2.3 have shown.

2.3 lightweight Cryptography

Lightweight cryptography is recently filed in the cryptography that is custom fitted resource constrained devices in IoT. Lightweight cryptography implies that are implemented in resource-constrained environments in IoT for encrypting and decrypting the data. Lightweight encryption is an intersection of two terms "Light and weight". Light and weight mean that are appropriate for less memory and fewer calculations require in IoT.

IMPLEMENTATION PLATFORMS	REQUIREMENT
HARDWARE	Chip area Energy utilization
SOFTWARE	Code size RAM/ROM capacity Computational power of micro processors and microcontroller

Table 2 Designing requirement of lightweight cryptography in IoT

Lightweight cryptography is likewise isolated into two type same conventional cryptography (1) symmetric cryptography (2) asymmetric cryptography (Public key Cryptography). Lightweight symmetric key cryptography works same as a conventional symmetric. Block cipher defined as "A block cipher takes a square of plaintext bits and produces a square of figure content bits, by and large of a similar size". A secret key is shared by at least two parties. Both parties can perform similar operations, such as encrypting and decrypting using same the key. Lightweight symmetric cryptography is more appropriate as the contrast with Public key Cryptography because of public key cryptography required complex calculations for key generations like RSA and so on.

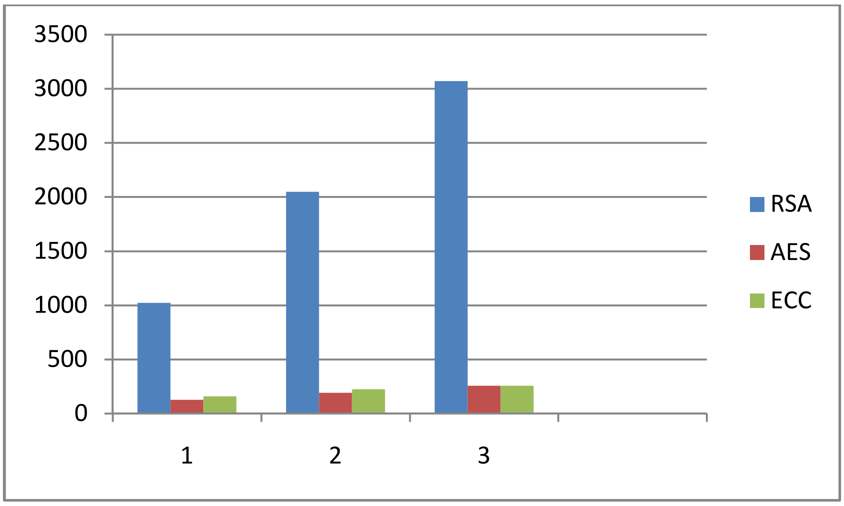

Fig.2.4 key size growth

RSA	AES	ECC	Key size Ratio (RSA:ECC)	Key size Ratio (RSA:AES)
1024	128	160	6:1	8:1
2048	192	224	9:1	10:1
3072	256	256	12:1	12:1

Table 3 comparable key size recommended by NIST of RSA and ECC/AES

Lightweight Asymmetric cryptography each party has a public and a private key. The private key is just known to its proprietor, while the general public key can be made accessible to everybody. This way all operations become asymmetric: rather than both sides having the capacity to register the encryption and unscrambling, just the proprietor of the private key can decrypt the message.Lightweight Asymmetric cryptography is more secure than.

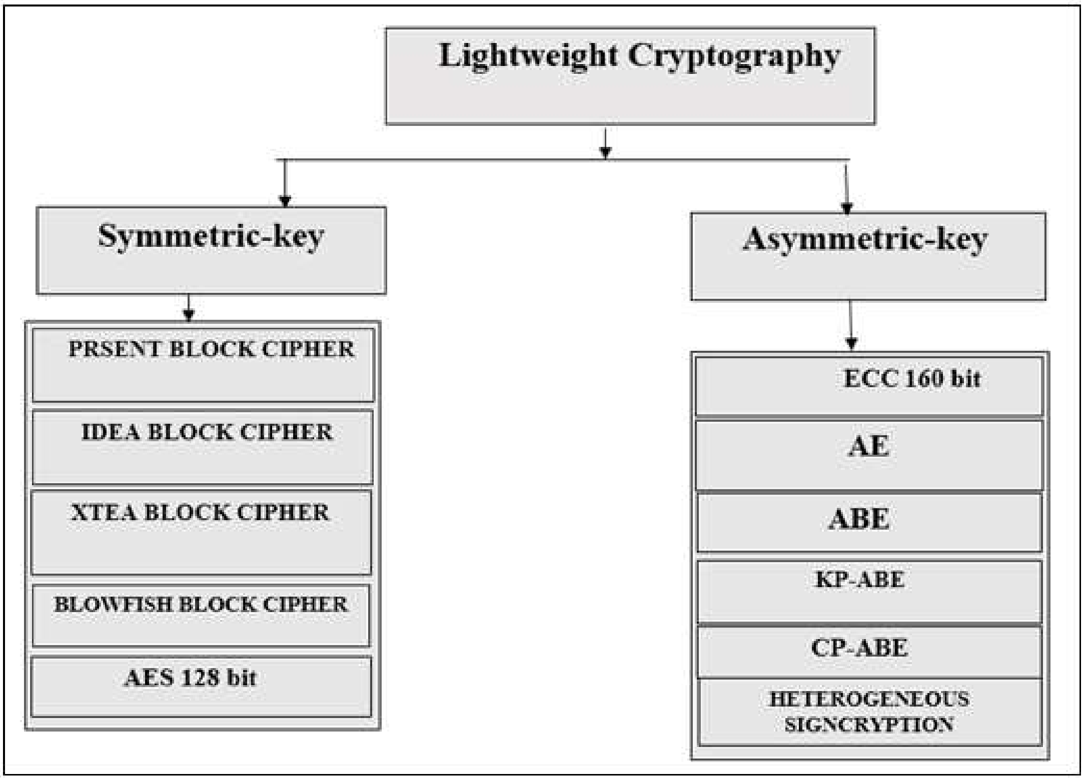

Fig. 2.5 Lightweight cryptography used in IoT

Lightweight symmetric cryptography in light of some lightweight symmetric block cipher is split like TEA and so forth. AES 128 bit is additionally lightweight symmetric encryption and decryption technique yet requires expressing key administration in IoT. In the Table 2 demonstrate some fundamental outlining necessities of Lightweight cryptography as far as hardware and software implementation.RSA encryption and decryption procedure are not appropriate in IoT environment because that constrained devices not handles huge key size. ECC 160 bit and AES 128 bit is appropriate for IoT environment. Table 3 demonstrate the key size that suggested by NIST. From the table 3 demonstrate that ECC and AES is utilized little key size for encryption and decryption process so AES and ECC is reasonable encryption methods in IoT in Figure 2.4 has indicated key size development of RSA and ECC/AES calculations.

Lightweight encryption is also two types

(i) Lightweight symmetric block ciphers.

(ii) Lightweight Asymmetric PKI.

Symmetric key

Lightweight symmetric key cryptography works same as conventional symmetric key. A block cipher characterized as "A block cipher take a plain content as info and block of cipher text bits".

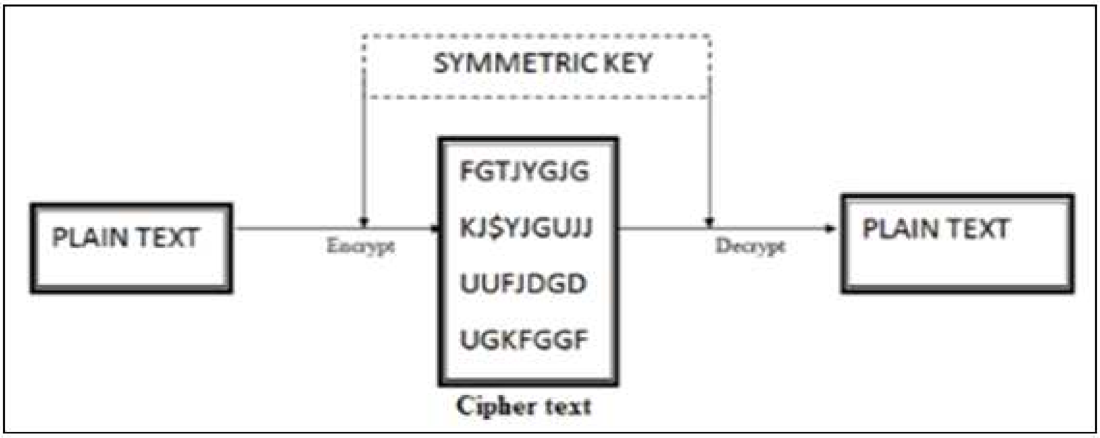

Fig. 2.6 Symmetric key

A secret key is shared by two or more parties. Both parties scan perform the similar operations, such as encrypting and decrypting utilizing the same key.

PRESENT BLOCK CIPHER

The present is an illustration of an SP-network [].Table 4 shows the rounds, block length and a key size of the present block cipher. Present cipher is suffered for collision problem if they used the bulk extent of date. Present cipher is mostly implementation on tag based devices.

Rounds	Block Length	Key size
31	64	80

Table 4 Present block cipher rounds block length key size

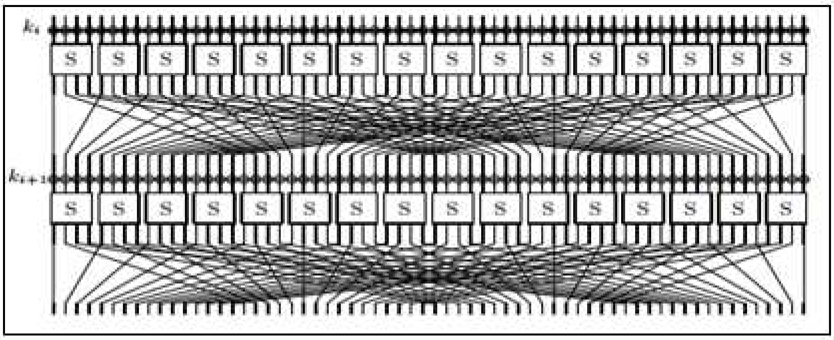

Fig. 2.7 Overview of Present Block Cipher [5]

IDEA BLOCK CIPHER

IDEA is a symmetric key encryption and decryption technique. Table 5 show block size and key size of IDEA.Fig.2.8 has shown Design method of IDEA symmetric cryptography.

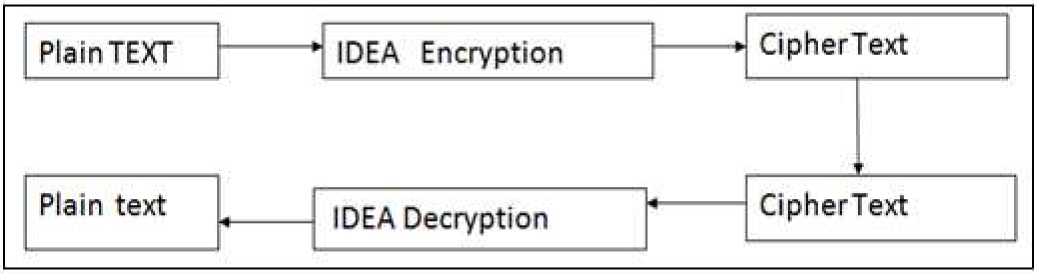

Fig. 2.8 IDEA Block Cipher Encryption and Decryption process

Three algebraic groups are being mingled, and they are all calmly implemented in both hardware and software.

Block	Key size
64	128

Table 5 show block size and key size of IDEA

XTEA BLOCK CIPHER

XTEA block cipher is part of the Tiny Encryption Algorithm to reduce the disadvantage of the TEA encryption. Tiny encryption algorithm ensures from the related key attack. Advantages of XTEA algorithm as a fellow XTEA algorithm hinges on a Feistel network with a variable bulk of rounds. XTEA encrypts an 8-byte text and craves a 16-byte key. The plaintext of the message M is divided into two bisects. Then in each round, the right side is first shifted left four and shifted right five. These two values are XORed with each other. The outcome is then added to the original right side first.

BLOWFISH BLOCK CIPHER

Blowfish, a block cipher is another very fast encryption and decryption technique as compare to IDEA and DES. Introduced by Bruce Schneier in December 1993.It is suitable where memory space is less than 5k.Blowfish block cipher is used simple operations for encryption and decryption process like addition, exclusive-or etc.Table 6 show block size and the key size of blowfish.

Block	Key size	Structure	Rounds
64 bits	32-448 bit	Feistel network	16

Table 6

AES BLOCK CIPHER

AES is a public key based encryption and decryption algorithm. The algorithm was proposed byJoan Diemen and Vincent Rijmen it also called Rijndael encryption and decryption technique. Table 7 shows The AES 128 bit Parameters. The encryption and decryption process of AES is divided into four key transformations has shown in Figure 2.9.

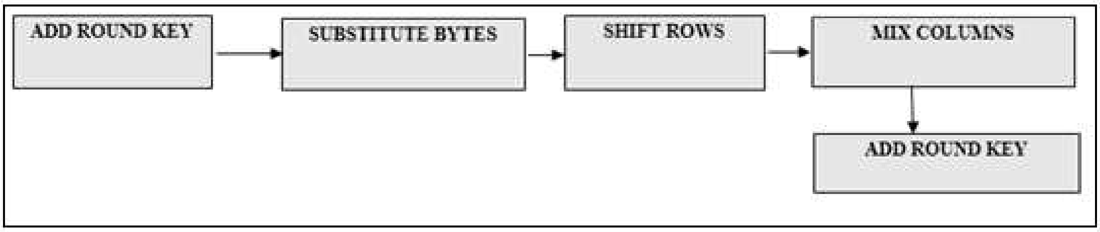

Fig. 2.9 four key transformations

AES encryption and decryption is pertinent lightweight encryption technique for IoT for encryption and decryption but requires explicit key management in IoT.

Key size (bits)	128 bit
Plaintext Block size (bits)	128 bit
Number of rounds	10
Round key size(bit)	128 bit
Expanded key size (bits)	44/176 bit

Table 7 AES 128 bit Parameters

Asymmetric PKI

In lightweight public key cryptography based on concept of two keys one is public and second is private key. The private key is only known to the receiver for decryption and public key is known to the sender for encryption public key can be made available to everyone. Encryption public key can be made accessible to everyone. In the Figure 2.10 show the show concept of lightweight asymmetric cryptography.

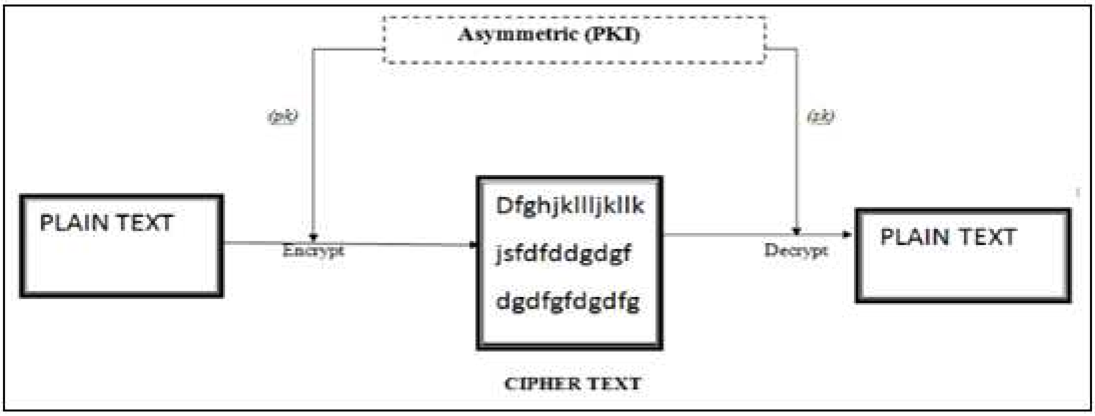

Fig. 2.10 Asymmetric PKI

This way all operations wind up plainly unbalanced: rather than both sides having the capacity to process the encryption and decryption, just the proprietor of the private key can decrypt the message. Asymmetric scheme consists of three algorithms:

(i) KeyGen (k).

(ii) Encrypt (E).

(iii) Decrypt (D).

The KeyGen (*k*) algorithm generates a public key *pk*and a private key sk.

Elliptic Curve Cryptography (ECC)

The concept of Elliptic Curve Cryptography (ECC) [4][5] was introduce by Victor Miller (IBM) and Neil Koblitz (University of Washington)in 1985. ECC is pertinent for IoT for secure the message transfer between send nodes to receiver ,ECC offer higher security for exchange the information over public network .It is based on public key infrastructure cryptographic approche,ECC used the, elliptic curve and ECDLP[]. Key size of ECC is 160 bit to 512 bit.

Algebraic Eraser

The establishment of the Algebraic Eraser public key cryptosystem together with its security lie in three distinct zones of mathematics: the hypothesis of braids, the hypothesis of matrices with polynomial sections (expressions of limited length developed from variable), and modular arithmetic in little finite fields. At its center is a very specific capacity (supplanting the standard framework's operations), known as E-Multiplication™, which unites these mathematical tools and empowers the framework to give rapid security without overpowering the memory and power accessible.

Attribute-based encryption

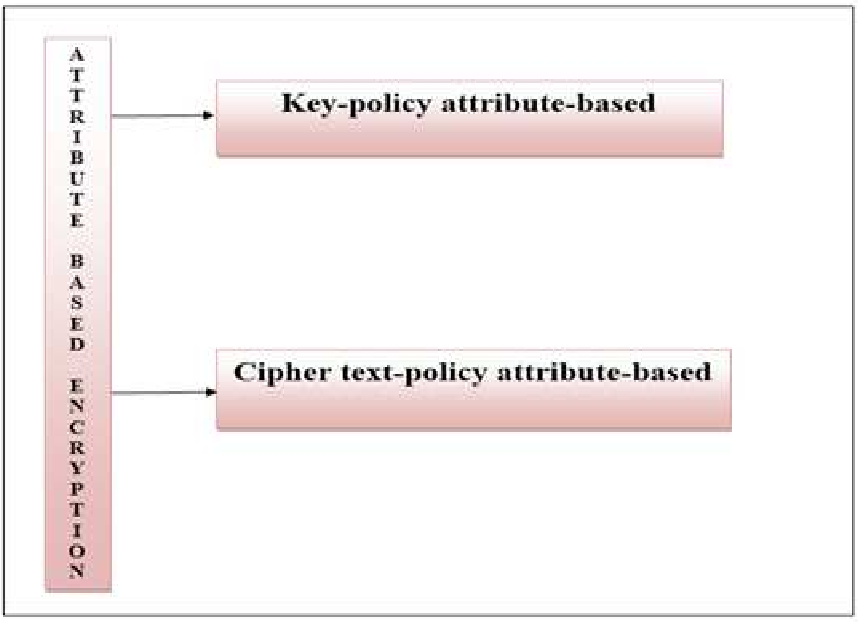

Fig. 2.11 Types of Attribute-Based Encryption

The concept of attribute-based encryption was first introduced in Advances in Cryptology EUROCRYPT 2005 [7]. ABE public key encryption and decryption technique is based on the set of attributes like email address and phone number etc. ABE cryptographic system is PKI based encryption and decryption technique combine the attribute with the attributes set for encryption and decryption. Figure 2.11 depicts the Types of Attribute-Based Encryption.

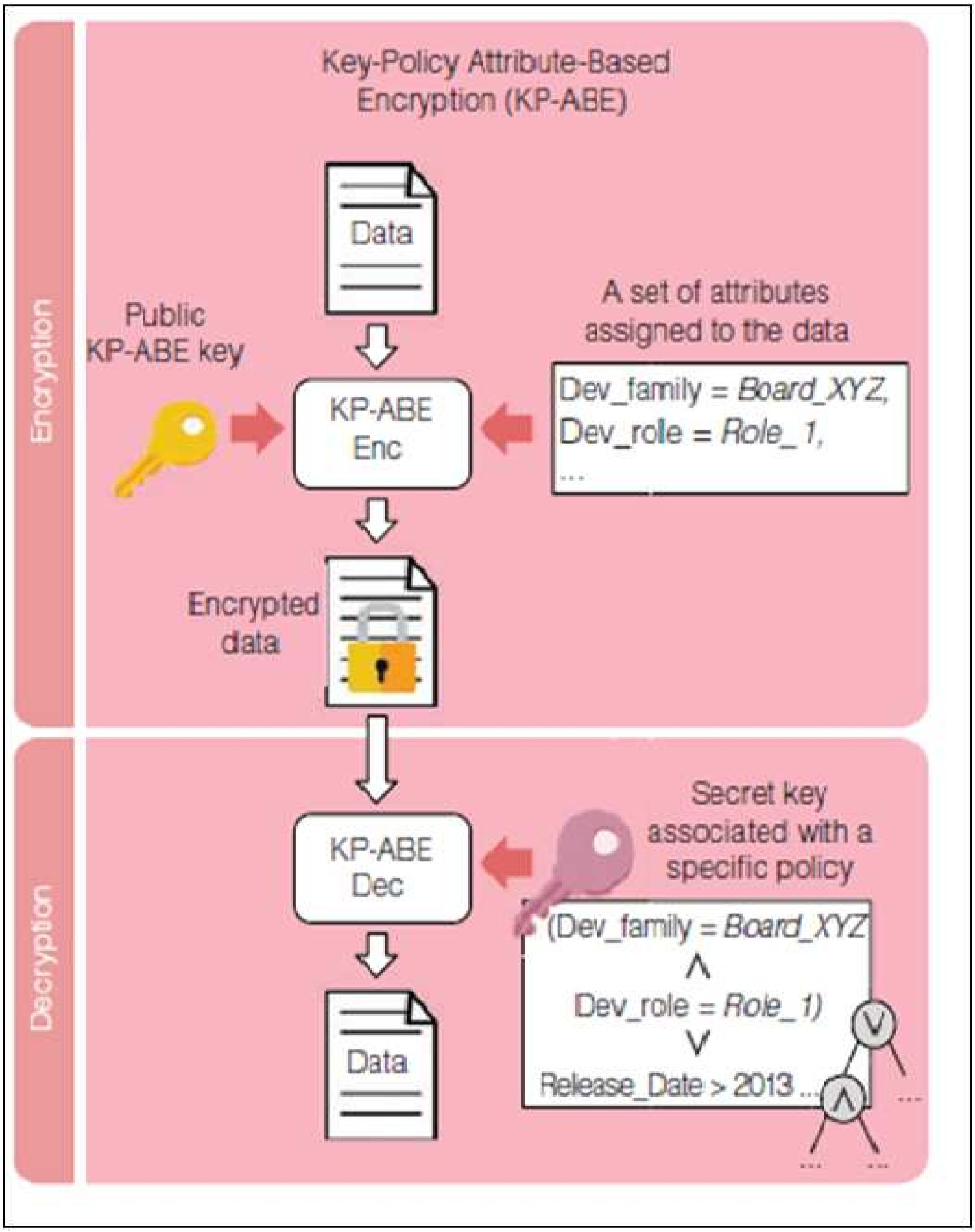

Fig 2.12 KP-ABE Process [3]

.

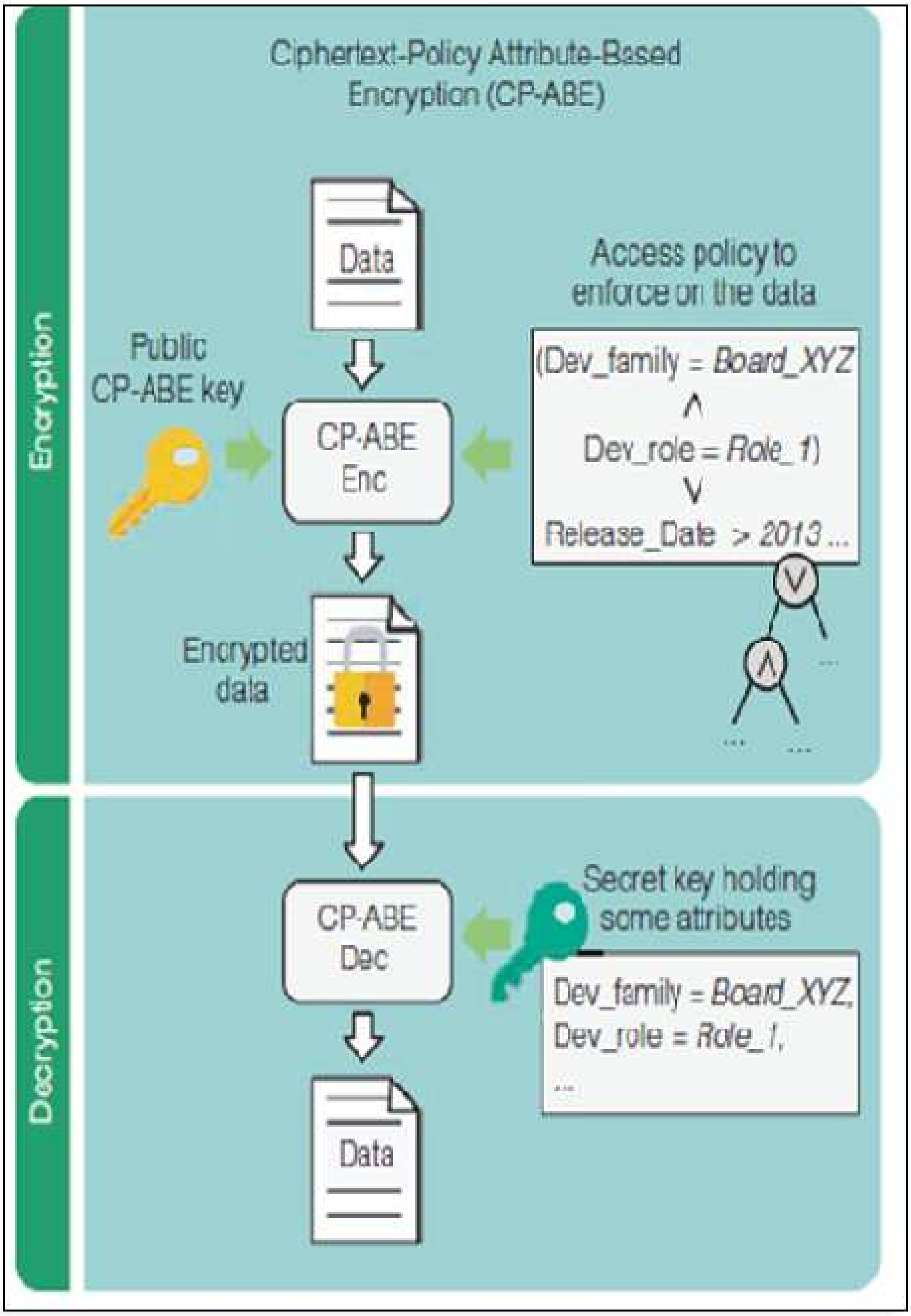

Fig. 2.13 CP-ABE [3]

AA-Beta (AAβ) encryption

In 2012 Ariffin proposed a AA-Beta(AAβ) encryption [].AA-Beta(AAβ) encryption is asymmetric cryptographic it is perform operation in three step .

(i) AAβ Key Generation.

(ii) AAβ Encryption.

(iii) AAβ Decryption

AAβ encryption times is good as compare to ECC the complexity is O(nlogn) for encryption and decryption is same as ECC decryption time is O(n2logn). 99% change on encryption time and change of 94% on decryption time for 2048-bit primes and Suitable for some applications.

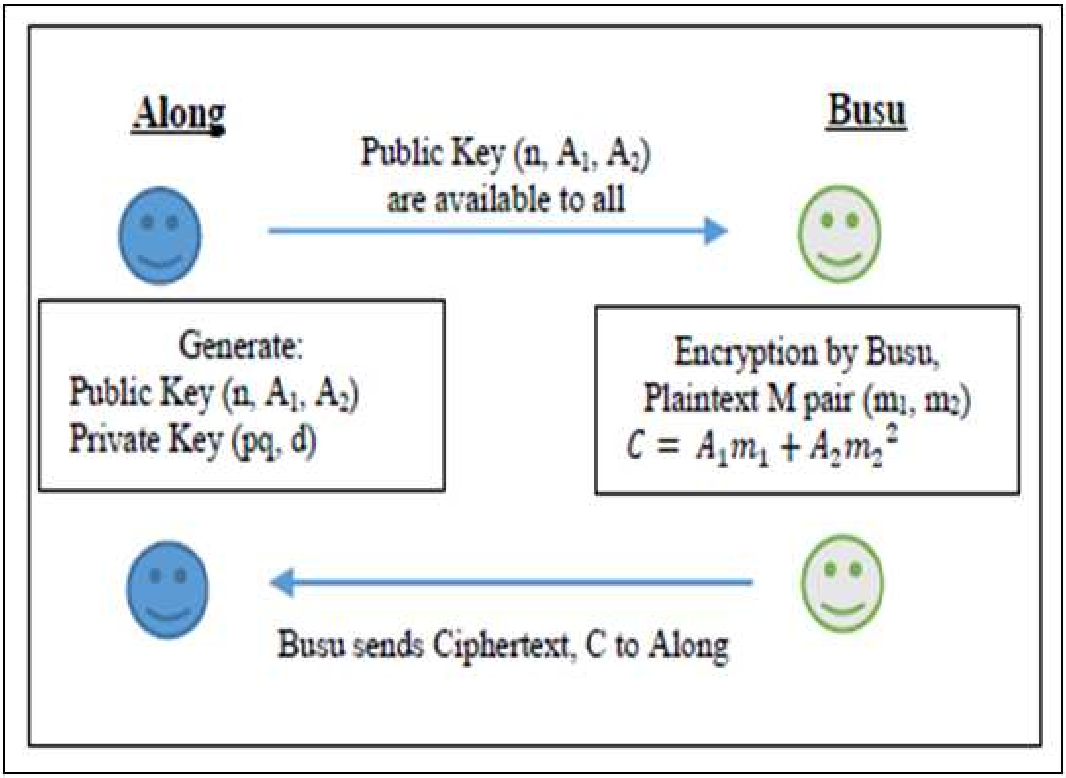

Fig .2.14 AAβ Encryption [19]

The encryption and Decryption has shown in figure 2.14 and 2.15

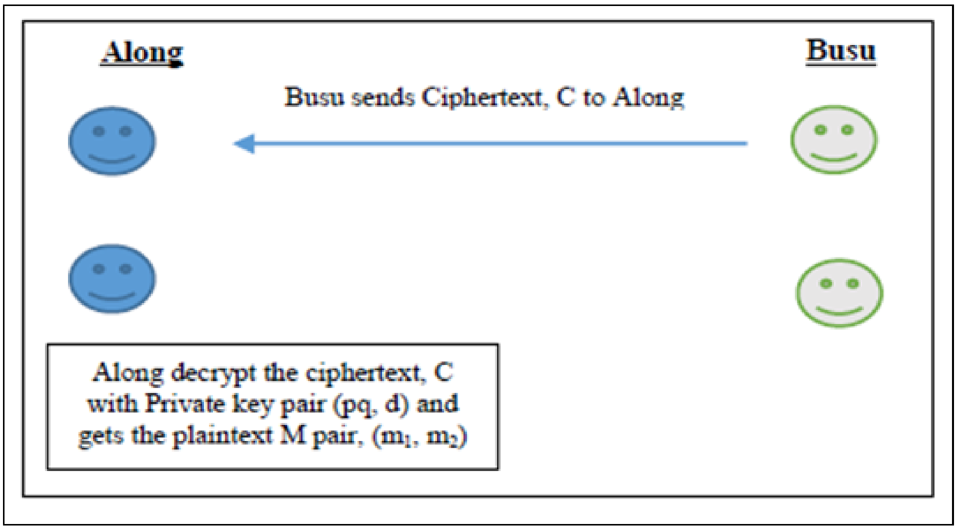

Fig. 2.15 AAβ Decryption [19]

Signcryption

In 1997signcryption [] Technique was proposed by Zheng. Signcryption is PKI based asymmetric cryptographic method that combines the digital signature and public encryption in single logical steps for providing secure communication at low cost.

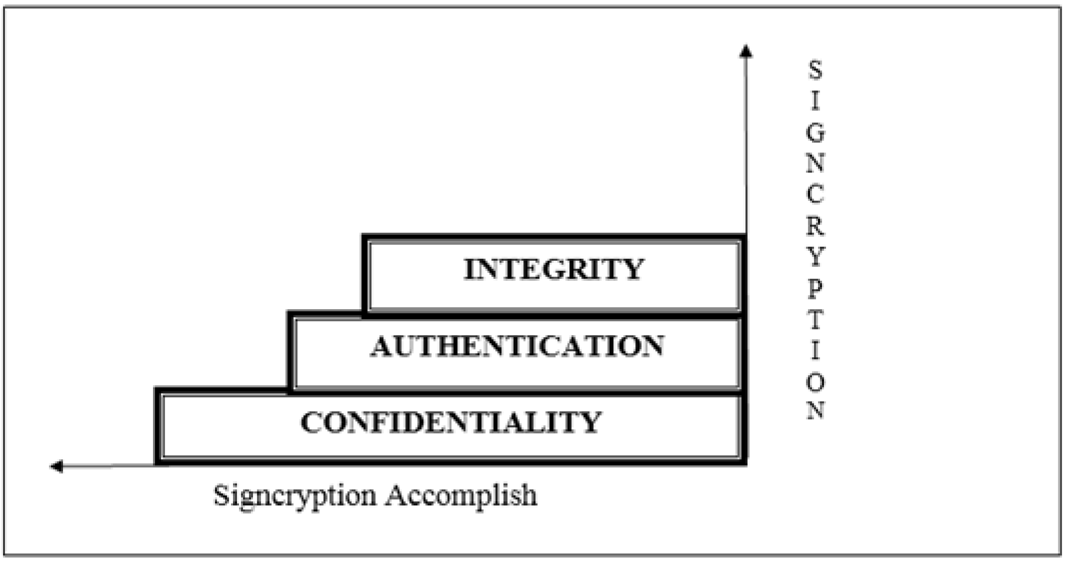

Fig.2.16 Advantage of signcryption accomplish in single logical step

Signcryption is pertinent for resource-constrained devices []. Advantage of signcryption has shown Figure.2 .16.

Requirement Lightweight Encryption in IoT

(I) Pertinent of devices-to-devices communication

(II)Pertinent to lower resource devices

Imperative Application of the lightweight cryptographic key algorithm allows lower energy consumption for end devices. Lightweight cryptography also delivers capable security.

2.4 Summary

IoT plays important role in day to day lifestyle. Various IoT applications improve the lifestyle of human in the earth. IoT is enduring from various security attacks. IoT attack divided into 5 types as fellow (1)Physical attack(2) Passive attack(3)Active attack (4) Attack on cryptography (5)Routing attack. Lightweight cryptography implies that is implemented resource-constrained environment in IoT for encrypting and decrypts the data. Lightweight symmetric cryptography is more reasonable as the contrast with Public key Cryptography because of public key cryptography required complex calculations for key generations like RSA and so on. Lightweight Asymmetric cryptography is more secure than Lightweight symmetric cryptography.

CHAPTER 3

Hardware Equipment

Chapter three discus the hardware equipment to established IoT environment. Figure 3.1 depicts the types of hardware equipment to set up the IoT environment.

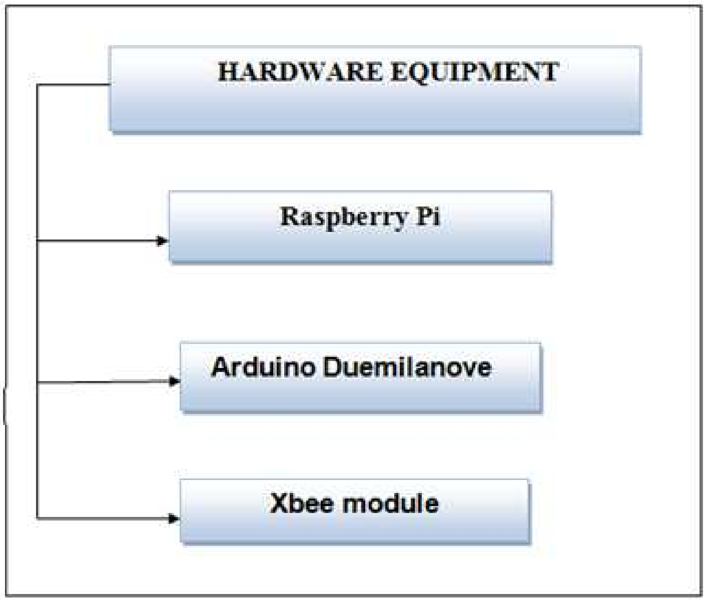

Fig.3.1 Types of hardware equipment

3.1 Raspberry Pi

Raspberry Pi (RPi) is a PC with charge card estimate additionally called SBC that includes Ethernet, USB and HDMI interfaces that can give top quality video and enough ability to run a Linux OS with GUI interface. Raspberry Pi has three model as fellow

- Model A
- Model B
- Model B+

All based in Broadcom BCM2835 SoC that gives a CPU, GPU, DSP, SDRAM and a single USB port. Table 8 depicts the characteristic Raspberry Pi all three model.

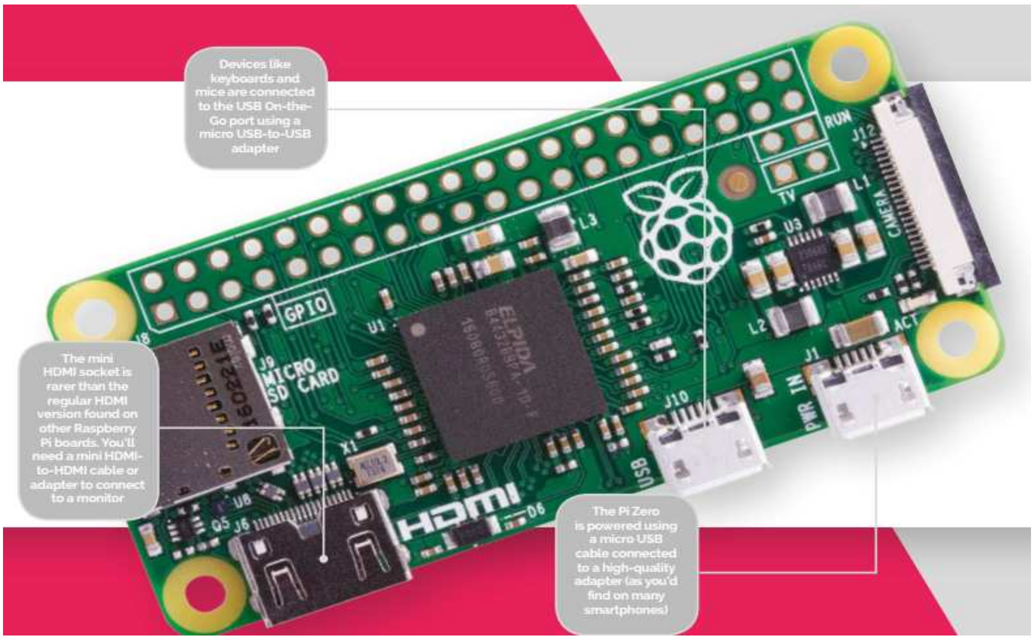

Fig. 3.2 Raspberry Pi [https://www.raspberrypi.org/magpi-issues/MagPi49]

Raspberry Pi Element	**Model A**	**Model b**	**Model B+**
SoC	Broadcom BCM2835	Broadcom BCM2835	Broadcom BCM2835
CPU	700 MHz ARM11 Family	700 MHz ARM11 Family	700 MHz ARM11 Family
GPU	Broadcom Video Core IV	Broadcom Video Core IV	Broadcom Video Core IV
Memory (SDRAM)	256 MB Shared	512 MB Shared	512 MB Shared
USB 2.0	1	2	4
Video outputs	Composite RCA and HDMI (rev. 1.3 and 1.4) PAL/NTSC	Composite RCA and HDMI (rev. 1.3 and 1.4) PAL/NTSC	Composite RCA and HDMI (rev. 1.3 and 1.4) PAL/NTSC
Audio outputs	3.5mm jack and HDMI	3.5mm jack and HDMI	3.5mm jack and HDMI
On board storage	SD / MMC	SD / MMC	MicroSD
Network	None	10/100 Mbit/s Ethernet	10/100 Mbit/s Ethernet
Power	300 mA (1.5W)	700mA (3.5W)	600mA (3W)

Table 8 Characteristic Raspberry Pi all three model.

3.2 Arduino Duemilanove

Arduino is a microcontroller board that makes conceivable to fabricate a infinity of DIY ventures with a minimal effort hardware. Table 9 depicts the characteristic of Arduino Duemilanove.

Microcontroller	ATmega168
Operating Voltage	5V
Input Voltage	7-12V
Interface	USB
Number of Digital I/O pins	14
Input pins	6
Flash memory	16 KB
SDRAM	1 KB
EEPROM	512 Bytes
Clock Speed	16 MHz

Table 9 Characteristic of Arduino Duemilanov

3.3 Xbee module

XBee modules offer wireless connectivity giving point-to-point, point-multipoint and mesh architectures XBee have two major families, XBee and XBee Genius, any family has distinctive types of antenna with different transmission power.XBee modules are intended to be utilized with Zigbee or IEEE 802.14.5 without compatibility one to each other. Table 10 depicts the characteristic of xBee pro.

Power supply	3.3V
Data rate	250kbps
Output	60mW
Range	1500m
ADC pins	6x10-bit
Digital IO pins	8

Encryption	128 bit

Table 10 characteristic of xBee pro.

3.4 Summary

In this chapter discus the different type hardware equipment to set up the IoT environment. Raspberry Pi has three Model A, Model B, Model B+ and explain the characteristic of various hardware equipment like a Raspberry Pi , Arduino Duemilanove and XBee modules etc.

CHAPTER 4

LITERATURE REVIEW

Chapter four is describe the literature review of few existing techniques that are suitable for encryption and decryption process in IoT environment.

4.1 Literature

A few kinds of existing techniques that are suitable for encryption strategy for IoT both in terms of hardware and software implementation and utilized for protecting data transmission in IoT are discussed here.

A. Bogdanovet al.in [15] Author introduce an ultra-lightweight block cipher that is appropriate encryption procedure for resource constrained devices. A present block cipher is depends on SP network [16].Present block cipher gave hardware productivity. However, utilized when application required direct security levels.

LyesTouati et al .in [17] Author introduce a cooperative ciphertext policy attribute encryption strategy as an option answers for securing information when information exchange over the public network from IoT end nodes. Deed the heterogeneous way of the IoT to make reasonable the utilization of the CP-ABE conspires in an IoT domain, exchange the task from exceedingly resource-constrained devices to hand over substantial operations in the CP-ABE plan to unconstrained nodes. The primary thought behind C-CP-ABE is to dispense calculation of CP-ABE encryption primitive, the resource–constrained protest can hand over the most devouring operations to unconstrained hubs of the system. The calculations of CP-ABE encryptions primitive is transposing from resource-constrained devices to unconstrained ones.

Ray Beaulieu et al. in [18] Author presents a lightweight block cipher. The hardware implementation of encryption and decryption process in IoT. SIMON and SPECK provided security on resource constrained devices in IoT environment. Reduce the circuit size.

Prasetyo et al. in [19] Author introduce a blowfish algorithm is implemented on FPGA utilizing VHDL programming language. Utilizing FPGA implementation is cheap, simple to execute, reprogrammed and high speed. Reduce the encryption time, give more prominent throughput and not influence avalanche effect significantly.

LyesTouati et al .in [20] Author proposed a solution does not include suspension resulting access grants and revocations. Discard the overhead subsequently of to re-encryption and renaming attributes and does not obligatory proxies to accomplish attribute revocations, dwindle to the negligible number of chunk created by the private key and does not incite any postponement. The creator proposed a Solution with impels zero delay and a negligible of produced secret key parts. The fundamental thought behind this arrangement is to gap time hub into schedule openings with variable period, Trusted Attribute Authority has not to rename ascribes keeping in mind the end goal to disavow them from a few clients, and has not likewise to recover all private key for all clients each property denial, it produces just lump of the private key applicable to a attribute.

Xuanxia Yao et al. in [21] Author proposed a lightweight no-pairing ABE method is based on elliptic curve cryptograph. The security of this strategy depends on ECDDH set instead of bilinear Diffie-Hellman posit, which can reduce the data processing overhead and communication overhead.ABE procedure design only for one specialist applications, it is not relevant to Ubiquitous IoT applications.

Mustafa Nawari et al. in [22] proposed a elliptic curve cryptosystem mellow by programming Spartan3E FPGA kit and analyzed by implementing Elgamla encryption plan on it.It contribute a similar level of the security that other surrogate contribute, it performs preparing in less time, less memory, less calculations and less power utilization. It is applicable for asset compelled gadgets in the IoT. Equipment usage of elliptic bend cryptography utilizing FPGA help the framework execution and a considerable measure of ensured than programming execution.

LyesTouati et al.in [23] Author present another procedure to reduces the complexity and the overhead, and does not require additional trust node in the system. In batch – based system that time axis is the separation into intervals of the similar duration that is called time slots, policy access to changes happens just between two successive time slots. Trust node passing only the vital attribute requires chunks every time slot to grant a thing to update its private key. Strategy has required synchronization between all things in the system. It doesn't necessary to re-encrypt data every attribute policy change. Batch- Based CP-ABE with Attribute Revocations Mechanism utilizing time slots idea.

T. Yalçin et al .in [24] Author proposed ECDSA for encryption and decryption process in IoT utilizing elliptic curve and digital signature algorithm. ECDAS motor is implemented an intellectual property (IP) in an 180 nm prepare This hardware encryption and decryption strategy.

LyesTouati et al.in[25] Author present KP-ABE scheme to utilize the computing power and storage capacity limit of cloud server and trust node for doing computations.

NouhaOualha et al. in [26] Author present CP-ABE construction utilizing effective pre-computation methods. The key idea driving pre-computation method is to pre-compute and store sets pair gathered with commonly exorbitant cryptographic operation. Pre-computation techniques based on the generator, the preprocessing algorithms of the generator are executed by the hardware devices or trusted authority. The pre-computation method reduces the cost of CP-ABE encryption, pre-calculation procedure utilized less calculation and less energy drain than original schema.

YijunMaoa et al. in [27] proposed a new FSFIBE procedure to ensuring information transmission in IoT. FSFIBE method is secure in the full model without random oracles. FSFIBE method has tight security reduction and a constant size of public parameters O (1).FSFIBE procedure gave the property of error-tolerance resistance. It is more related for securing IoT communications.

Fagen Li et al.in[28] Author propose a heterogeneous ring signcryption procedure for secure communication from resource constrained devices to a server over public system. The heterogeneous ring signcryption system declare sender in IBC environment to send a message to a receiver in the PKI domain. The strategy at the same time obtains confidentiality, integrity, authentication, non-repudiation and anonymity in a sensible single step.

Kun-Lin Tsai et al. in [29] Author proposed the third party based multi-key exchange protocol and utilize elliptic curve encryption and decryption. Secure against five assaults (Replay assault, Eavesdropping assault, Known-key assault, Impersonation assault, Forgery assault).

Syed Farid Syed Adnan et al .in [30] Author introduce an examination of lightweight asymmetric encryption, the AAβ (AA-Beta).That might be practically in IoT. 99% change on encryption time and change of 94% on decryption time for 2048-bit primes.

Hague-Chung et al .in [31] Author present a protocol for low power and low speciation devices communicate utilizing client smart devices through gateway and certificate authority. This protocol gives insurance shape re-use assault and center assault.

Ref No	**Techniques Used**	**pros**	**cons**
[15]	SP-network single 4-bit to 4-bit S-box	Hardware efficiency	Implemented in hardware Moderate security levels
[17]	C-CP Attribute-based Encryption	Feasible Efficiently Security	Trusted unconstrained nodes in its neighborhood
[18]	SIMON AND SPECK ALGORITHMS SIMPLE round functions XOR ,AND, Not	Reduce circuit size	Implemented in hardware
[19]	BLOWFISH ALORITHM on FPGA	Reduce total encryption time	Costly. Required hardware.
[20]	Efficient CP-ABE/Key Management	Reduces the complexity and The overhead.	Not required extra trust nodes
[21]	No-pairing ABE	Reduce the processing	Not pertinent to Ubiquitous

	technique based on elliptic Curve cryptograph	overhead And communication Overhead.	IoT applications
[22]	FPGA based Implementation of elliptic curve Cryptography	Less memory. Less computations, Security	Costly. Required hardware
[23]	Batch-BASED CP-ABE with Attribute Revocations	policy access changes occur only between two successive time slots. .	Need synchronization
[24]	Elliptic curve digital signature algorithm	Intellectual property (IP)in a 180 nm process Dual-port memory support	Costly SUTIABLE FOR HARDWARE IMPLAMATIONS
[25]	KP -ABE and cloud servers and resource constrained node	Complex operations of the encryption and decryption process pass to trusted unconstrained assistant nodes and a cloud server.	Each resource constrained device contain at least two trusted unconstrained devices in its neighborhood
[26]	Pre-computation techniques using ECC	Encryption does not require scalar point multiplications less energy consuming.	Storage
[27]	Fuzzy identity-based encryption	Secure in the full model without random oracles	Enlarge Key size
[28]	Heterogeneous ring signcryption technique	Confidentiality, Integrity, Authentication	Bilinear pairings
[29]	Multi-Key Exchange Protocol Using ECC	Achieves fully mutual authentication. security level and performance are higher	Overhead increasing

[30]	Lightweight AAβ Encryption Scheme	99% change on encryption time and change of 94% on decryption time for 2048-bit primes.	Suitable for some applications
[31]	CA and gateway	safe, and it protects the re-use attack and middle attack	Mutually safe procedure,

TABLE 11. COMPARISON BETWEEN RELATED WORKS

4.2 Summary

Some techniques reduce the complexity overhead and some reduce the processing overhead and communication overhead. Some of the techniques used trust nodes in its neighborhood for doing computation operation of constrained Devices. When implemented encryption and decryption technique in terms of hardware computations is fast but chip size increasing and in terms of a software implemented computations is slow but required small code size. Some of the technique is provided more security but performance is less and cost is high.

CHAPTER 5

Proposed Solution

In this solution is to design intelligent gateway with notarization security system for execution encryption and decryption strategies in term of software implementation for class-0 devices. In this arrangement intelligent gateway which endow data aggregation and filtering of data. Notarization security component set up the trust third party for generating the public and private key for encryption and decryption for class-0 devices. Proposed solution is pertinent for small scale applications in IoT like smart school, rural management systems etc.

5.1 Proposed IoT Security architecture

Figure 5.1 has shown Proposed IoT security architecture for IoT. Proposed architecture partition into four layers as fellow

- Physical layer,
- Commutation layer,
- Data collaboration management layer,
- Application layer.

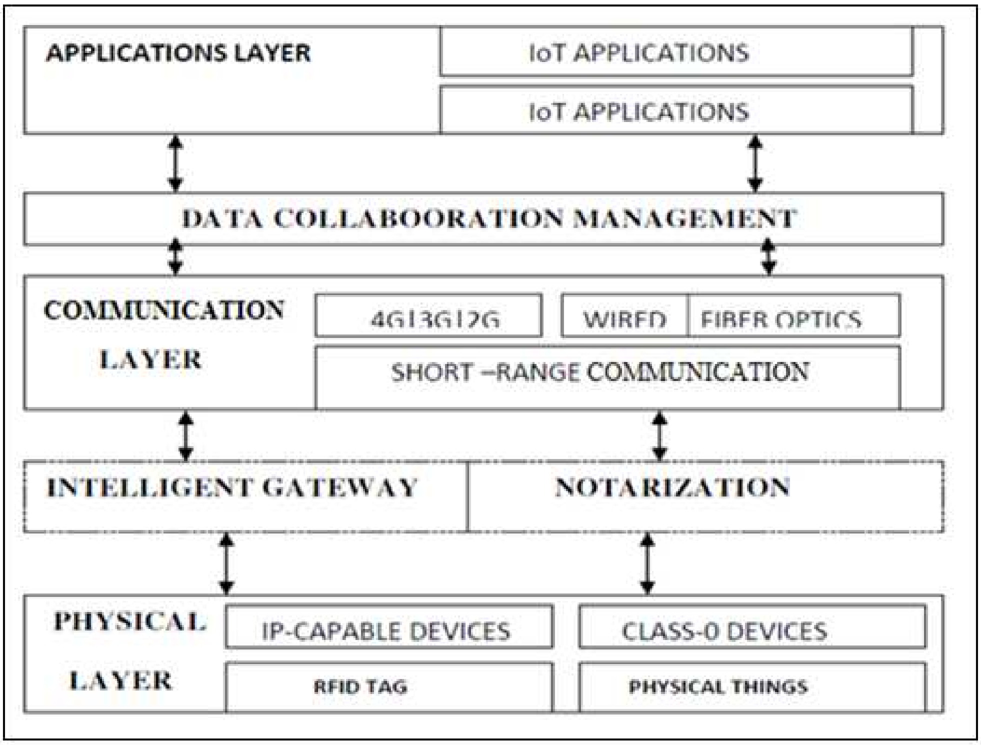

Fig. 5.1 Proposed IoT Security Architecture

Physical layer

The first layer is physical layer (also called perceptual layer) is in charge of assembly data for each things(object) and consist of constrained devices and unconstrained devices.

Intelligent Gateway

Intelligent gateway [] perform an operation like aggregation, filtering of data etc. data collected from the various heterogeneous nodes in IoT. This data is collected by constrained devices like sensor's and passes to the intelligent gateway to perform an operation of data aggregation and data filtering.

NOTARIZATION

Notarization intends to set up trust third party mechanism for encryption and decryption process for information gathered by the physical layer and key administration functions. Notarization mechanism performs all complex operation of encryption and decryption process. Figure 5.2 depicts the notarization mechanism.

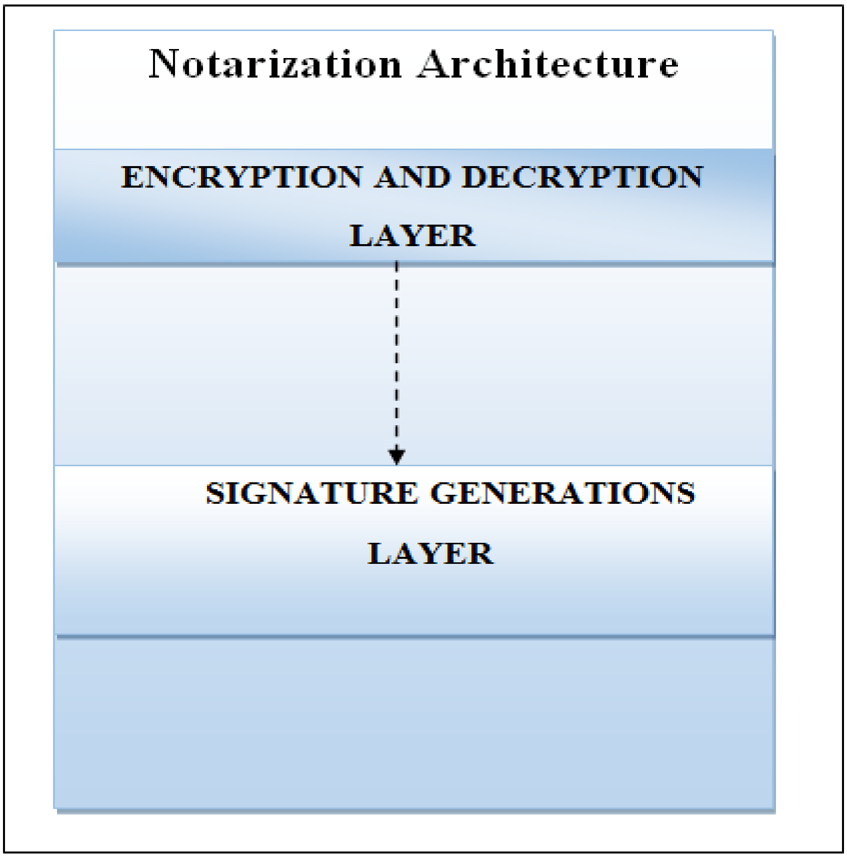

Fig. 5.2 Notarization Architecture

Notarization mechanism architecture divides into two layers. The first layer is encryption and decryption layer which responsible for generating the public and private key for encrypt and decrypt the data gathered by the physical layer and consist of lightweight encryption and decryption algorithms. The second layer is signature generation layer that is in charge of producing the digital signature for purpose of data integrity.

Communication layer

The Communication layer that is capable of transmitting the data assembly from the physical layer. While the transmission media like as 4G,3G,2G, wireless, wired, fiber-optic, short range communications for commutating the data over a public network.

Data collaboration management layer

Data collaboration management layer is managing data storage and database. Data collaboration management layer handle the all database operations like data storage and data base management systems etc.

5.2 Proposed Approached

The proposed solution utilized AES 128 bit lightweight symmetric encryption and decryption system to Encrypting and decrypting the data gathered by the constrained and unconstrained devices used in IoT environment.

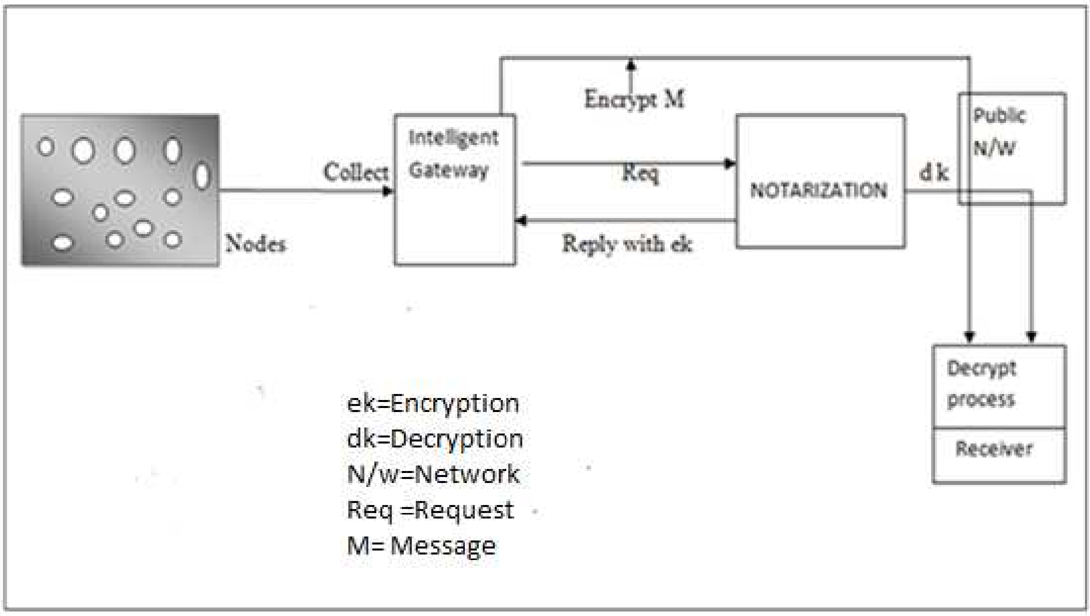

Fig. 5.3 Proposed Approached

ECC-160 bit lightweight asymmetric encryption and decryption strategy utilized for a reason for producing the digital signature for giving information respectability. Figure 5.3 depicts the working of the proposed approached. In this approach data is collected by an intelligent gateway for performing data conglomeration operation for aggregate the data come from various heterogeneous nodes. Notarization mechanism generating encryption key ek and send to the client for encrypt the collected data and send over a public network.

Lightweight Encryption And Decryption	**Parameter**	**Technique**	**Pros**	**cons**
Lightweight attribute-based encryption for the Internet of Things.[21]	Communication overhead. Computational overhead.	No-pairing ABE schema based on ECC.	Execution efficiency. Low communication cost.	Flexibility in revoking to attribute. Generality. Scalability.
C-cp-abe: Cooperative ciphertext policy attribute-based encryption for the internet of Things [17].	Reduce the induced overhead at resource constrained devices.	Third party feasible the implementation of CP-ABE	Less energy consuming than the original CP-ABE Schema.	Require unconstrained node in its neighborhood
Batch-Based CP-ABE with attribute revocation mechanism for the internet of Things [23].	Traffic	Batch-Based CP-ABE	Does not require re-encrypting data every attribute policy change.	Cause of delay

Lightweight Attribute-Based Encryption for the Internet of Things [26].	Energy saving	Pre computation	Feasible implementation of CP-ABE	Storage
Collaborative KPABE for cloud-based internet of things[25]	Computing power Storage capacities	Used cloud server Trusted assistant node	Heavy operation of encryption and decryption done by turst un constrained and cloud server	Require at least two trusted un constrained.
Secure and efficient data transmission in the Internet of Things[]	Confidentiality Integrity Authentication Computation time	Heterogeneous ring signcryption	Avow sender in the IBC environment to send a message to a receiver in the PKI domain	Not suitable for large scale network
lightweight AAβ encryption scheme[]	Flexibility Scalability	AAβ encryption and decryption	99% change on encryption time and change of 94% on decryption time for 2048-bit primes	Suitable for only embedded devices that support Linux real time operating system

Table 12 compressive study with parameter.

Notarization also generating the decryption key for decrypts the data and send to the receiver (laptop, server Smartphone). A sender is comprised of resource-constrained devices that are not skilled for computation or storage. In Our Proposed Approached first compare a few lightweight encryption techniques that are pertinent in IoT. A table 12 shows few lightweight encryption techniques compressive study with parameter.

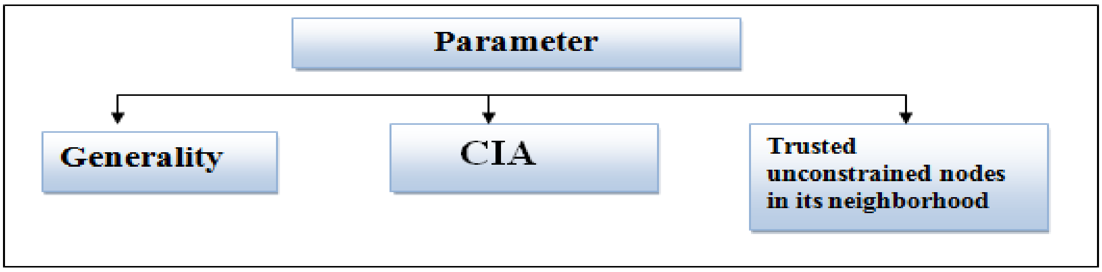

Fig. 5.4 Considered parameter in a proposed approached

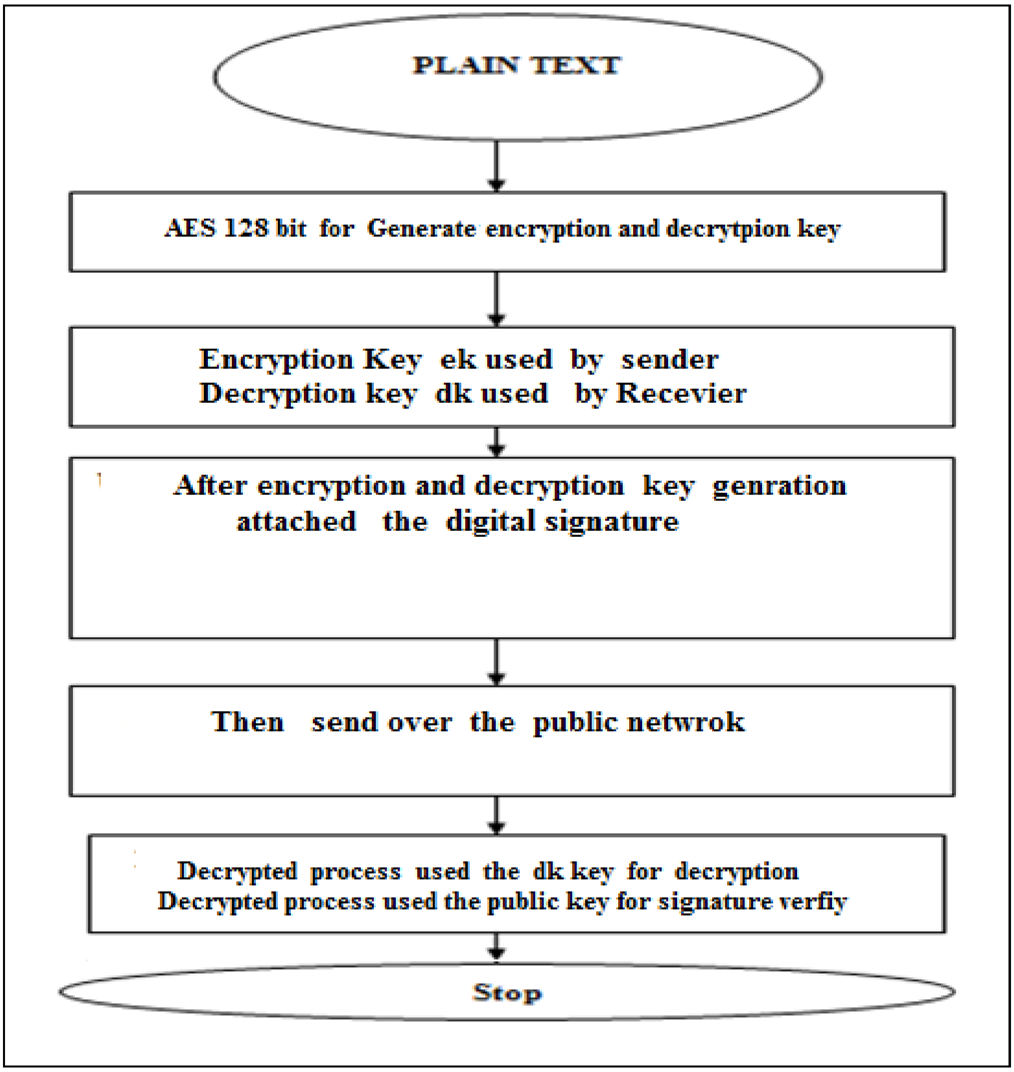

Fig. 5.5 Flow diagram

Proposed Technique Steps for encryption and decryption process

In this technique consider two phase use Figure 5.6 depicts.

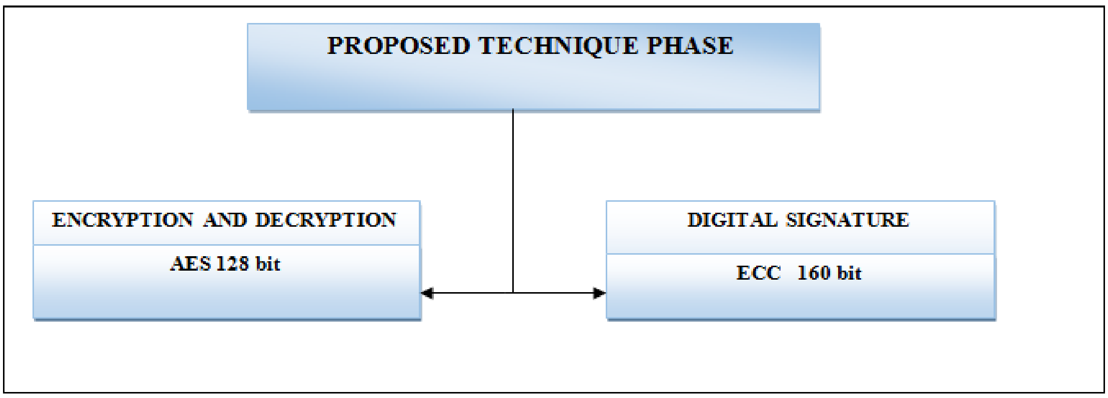

Fig. 5.6 Proposed Technique Phase

First phase consider the AES 128 bit encryption and decryption process for generating key for encrypted and decrypted data. Second phase consider the digital signature generation.

Step 1	Derive the set of round keys from the cipher key.
Step 2	Initialize the state array with the block data (plaintext).
Step 3	Add the initial round key to the starting state array.
Step 4	Perform nine rounds of state manipulation.
Step 5	Perform the tenth and final round of state manipulation.
Step 6	Copy the final state array out as the encrypted data.

Fig .5.7 Encryption steps

Step 1	**Initial decryption round:** XorRoundKey InvShiftRows InvSubBytes
Step 2	Perform nine full decryption rounds: XorRoundKey InvMixColumns InvShiftRows InvSubBytes
Step 3	Perform final XorRoundKey

Fig .5.7 Decryption steps

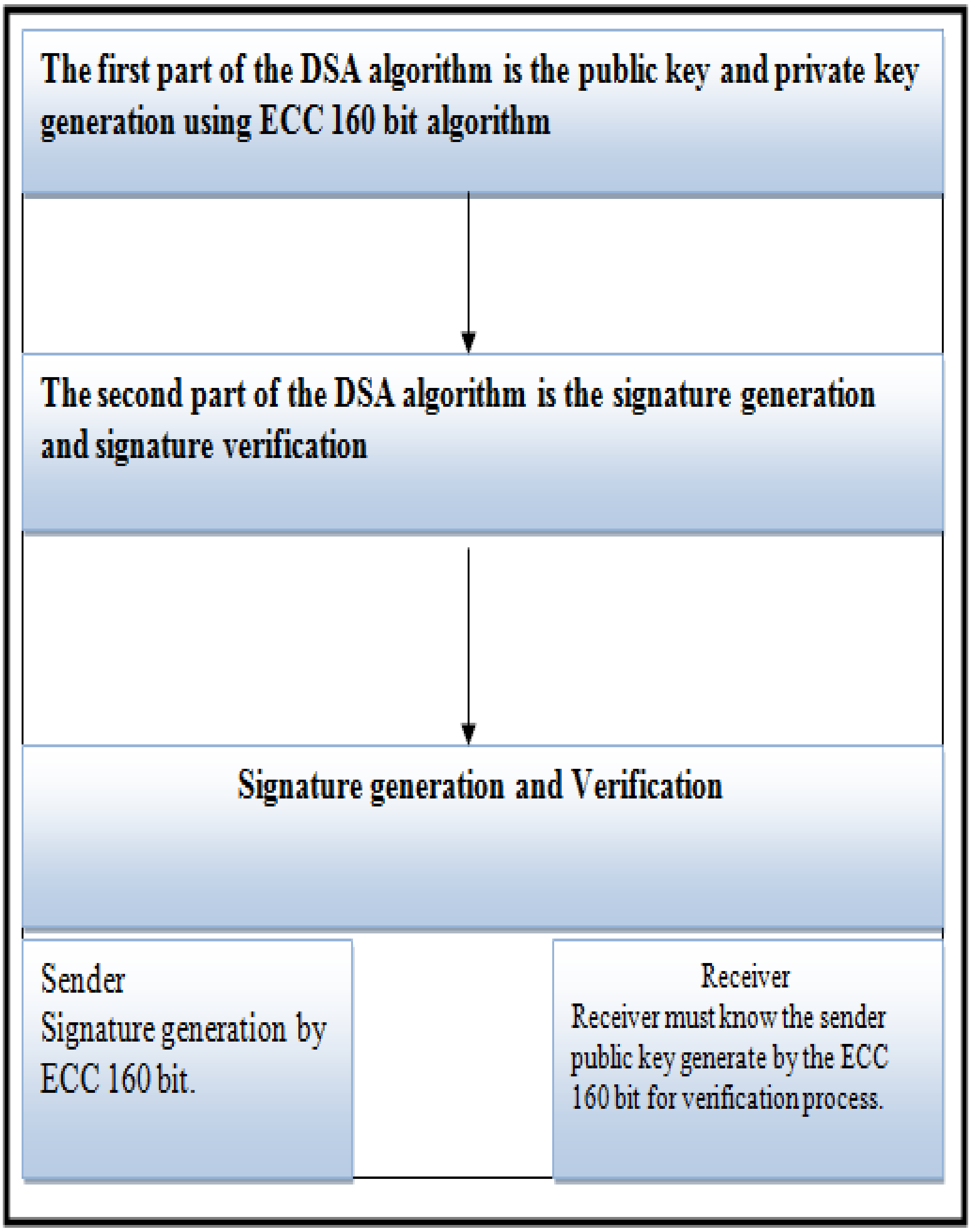

Fig. 5.8 digital signature process step

5.3 Summary

Solution is to design intelligent gateway with notarization security system for execution encryption and decryption strategies in term of software implementation for class-0 devices. Notarization security component set up the trust third party for generating the public and private key for encryption and decryption for class-0 devices. Proposed Approached first compare a few lightweight encryption techniques that are pertinent in IoT.

CHAPTER 6

Implementation and Result Analysis

We implemented notarization strategy utilizing java micro edition software development kit that gives the adaptable condition to an application running on resource-constrained devices in IoT.

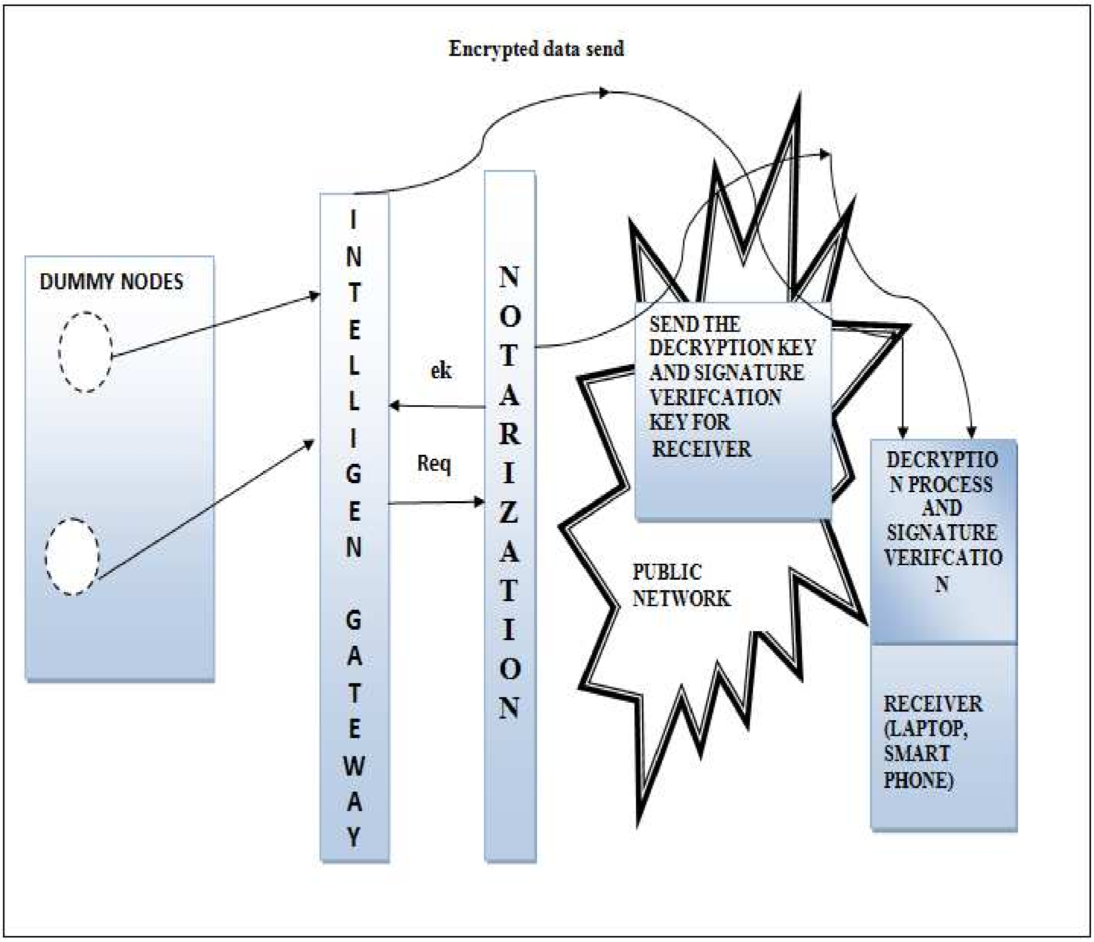

Fig.6.1 Block diagram of our Implementation proposed technique.

In our experiment, we outline two dummy and one master node and the server node. Master node gathered the aggregated information from an intelligent gateway and produces the key for encryption and decoding and the digital signature for enhancing the security in IoT environment. Master node sends the decryption key to the server for decoded data. Block diagram of our Implementation proposed technique has shown in figure 6.1.

6.1 Result Analysis

Table 13 present the comparison parameter of various key exchange techniques and our proposed hybrid encryption and decryption using notarization. Figure 6.2 has shown the encryption and decryption time proposed by our technique.

Proposed Technique	Encryption time	Decryption time
HEDUN	433 ms	437ms

Table 13 encryption and decryption time of HEDUN technique in millisecond

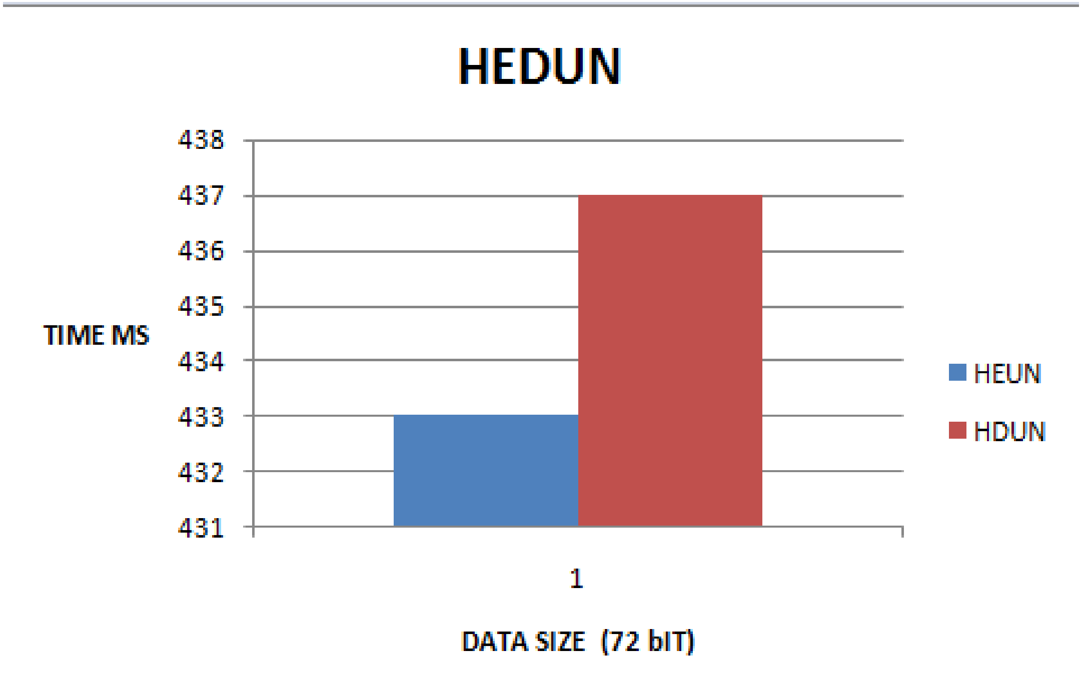

Fig. 6.2 Proposed HEDUN time using notarization

Table 14 has shown encryption time and decryption time in ms of RSA using notarization. In this experiment we have using non lightweight encryption and decryption technique using RSA. And compare with our proposed technique using lightweight AES 128 bit for encryption and decryption and ECC 160 bit for generating digital signature and see the time difference between our proposed technique and RSA using notarization mechanism .Figure 6.3 depicts the time difference.

Cryptography algorithm	Encryption time	Decryption time
RSA 512 bit	1970 ms	2650 ms
RSA 1024 bit	2415 ms	2997 ms
RSA 2048 bit	4025 ms	4835ms

Table 14 Encryption time and decryption time in ms of RSA using notarization

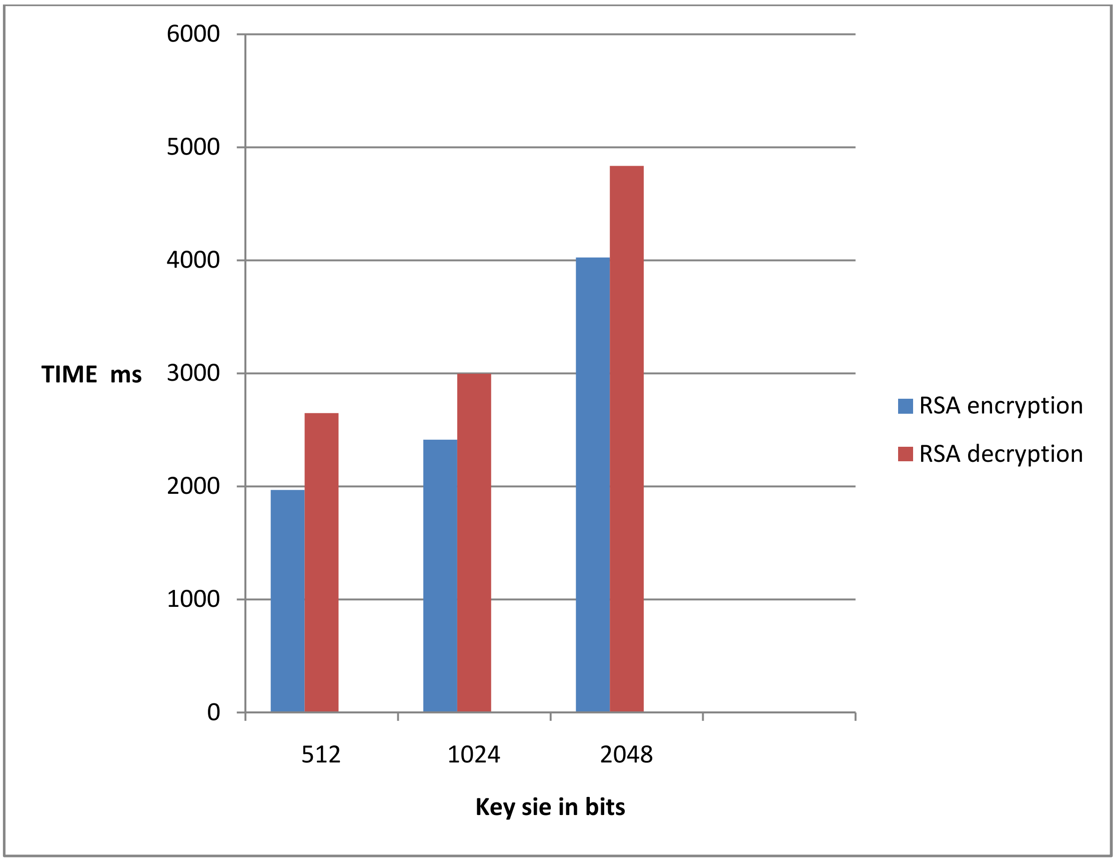

Fig. 6.3 time difference of RSA using notarization

Table 15 has shown encryption time and decryption time in ms of IBE using notarization mechanism. In this experiment we have using encryption and decryption technique IBE using the RSA 2048 bit for encryption decryption process used by notarization for generating the key. And compare with our proposed technique see the time difference between our proposed technique and RSA using notarization mechanism .Figure 6.4 depicts the time difference.

IBE using RSA 2048	Encryption time	Decryption time
IBE	2890 ms	2967 ms

Table 15 has shown encryption time and decryption time in ms of IBE using notarization mechanism

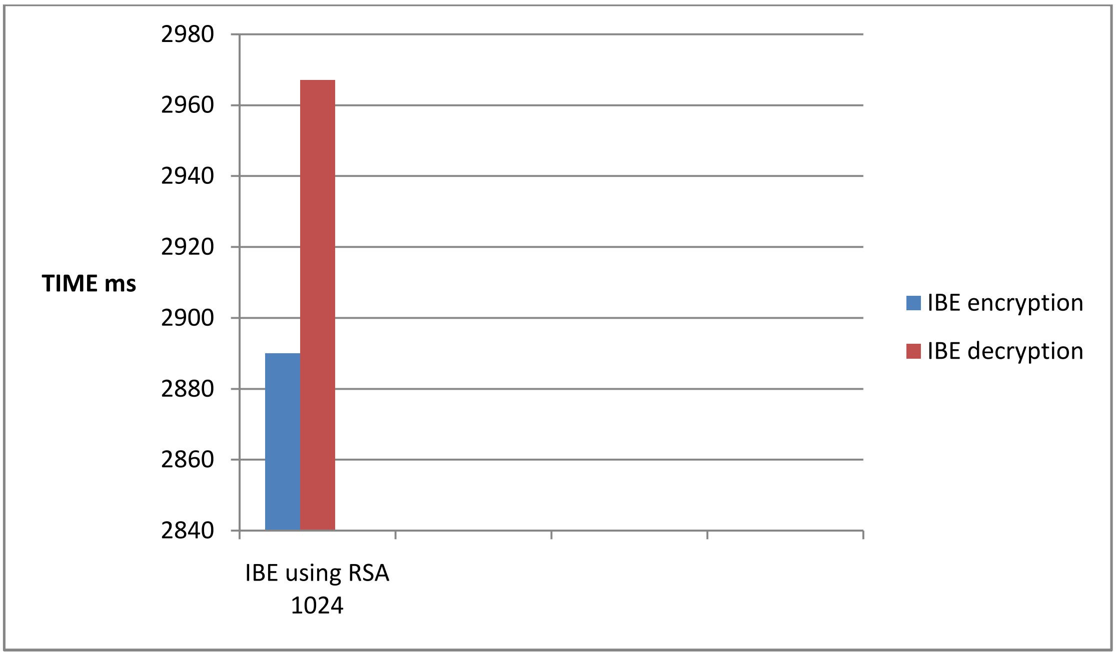

Fig .6.4 Time difference of RSA using notarization

Comparison Parameter	Touati[17]	Xuanxia[21]	HEDUN[Proposed]
Trusted unconstrained nodes in its neighborhood	Yes	No	No
Single authority application	No	Yes	No
Computation Time	Low	Low	Moderate
CIA	confidentiality	confidentiality	Confidentiality/Integrity
Cryptographic types for key generations	Asymmetric type	Asymmetric type	Symmetric type

Table 16 Comparison table of existing and proposed approaches

Table 16 presents the comparison of existing and proposed approaches against numerous parameters such computation time, trust factor and cryptographic needs.

6.2 Summary

In this chapter perform a experimentally analysis of a proposed approached and RSA encryption and decryption and IBE encryption and decryption technique using notarization mechanism and See the time take by encryption and decryption process and comparison of existing and proposed approaches against numerous parameters such computation time, trust factor and cryptographic needs.

CHAPTER 7

Conclusions and Future work

Chapter seven concluded the thesis and discusses future work related to this proposed approached. Section seven is isolated into three section initially contain conclusion of the thesis and last section clarify the future work and.

7.1 Conclusions

The aim of this thesis is identify the various lightweight encryption and decryption techniques and perform an experimentally analysis. In this thesis mainly focused on the different lightweight encryption and decryption technique used in IoT for secure data transmission and enhance the security of IoT. In this thesis, explained various security attack and importance of IoT in a day to day. Every technique has some advantages and disadvantage in IoT. Some technique required more storage space but less computation vice versa. In this thesis compare research status of various lightweight encryption and decryption in IoT. Conventional internet is different form IoT, conventional internet is rich in its power resource, memory, storage etc.where IoT is less power, memory, and storage. In thesis is tried to find the best lightweight encryption and decryption using the notarization mechanism. In this thesis proposed a security mechanism using third party trust for do the complex operation of encryption and decryption process for key generation and compare the encryption and decryption time of RSA encryption and decryption and IBE using notarization mechanism and compare with our proposed technique and also do the comparative study of exiting lightweight encryption technique that are suitable for IoT.

7.2 Future work

In this thesis we try to find the best encryption and decryption technique that required less time for encryption and decryption in IoT. In our proposed technique required to improve the encryption and decryption time that may practical suitable for IoT. Identify vulnerabilities in the proposed technique strategy and discover answers for them before usage.

Hopefully this research work can providing the basic idea of encryption and decryption techniques that are used in IoT and guideline for the research related to encryption and decryption in IoT.

References

Journal

[1] Ashton, K., 2009. That ‘internet of things’ thing. *RFiD Journal*, *22*(7), pp.97-114.

[2] Jang, Seiie, and Woontack Woo. "Ubi-UCAM: a unified context-aware application model." In *International and Interdisciplinary Conference on Modeling and Using Context*, pp. 178-189. Springer Berlin Heidelberg, 2003.

[3] Li, Yang, Mengting Chen, and Jian Wang. "Introduction to side-channel attacks and fault attacks." In *Electromagnetic Compatibility (APEMC), 2016 Asia-Pacific International Symposium on*, vol. 1, pp. 573-575. IEEE, 2016.

[4] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "A Lightweight Trust Design for IoT Routing." In Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016 IEEE 14th Intl C, pp. 552-557. IEEE, 2016.

[5] Dalipi, Fisnik, and Sule Yildirim Yayilgan. "Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges." In *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on*, pp. 63-68. IEEE, 2016.

[6] Al Salami, Sanaah, Joonsang Baek, Khaled Salah, and Ernesto Damiani. "Lightweight Encryption for Smart Home." In Availability, Reliability and Security (ARES), 2016 11th International Conference on, pp. 382-388. IEEE, 2016.

[7] Jara, Antonio J., Latif Ladid, and Antonio F. Gómez-Skarmeta. "The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities." *JoWua* 4, no. 3 (2013): 97-118.

[8] Islam, SM Riazul, Daehan Kwak, MD Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. "The internet of things for health care: a comprehensive survey." *IEEE Access* 3 (2015): 678-708.

[9] Bhunia, Swarup, Michael S. Hsiao, Mainak Banga, and Seetharam Narasimhan. "Hardware Trojan attacks: threat analysis and countermeasures." *Proceedings of the IEEE* 102, no. 8 (2014): 1229-1247.

[10] Bertino, E. and Islam, N., 2017. Botnets and Internet of Things Security.*Computer*, *50*(2), pp.76-79.

[11] Ngai, Edith CH, Jiangchuan Liu, and Michael R. Lyu. "On the intruder detection for sinkhole attack in wireless sensor networks." In*Communications, 2006. ICC'06. IEEE International Conference on*, vol. 8, pp. 3383-3389. IEEE, 2006.

[12] Zhang, K., Liang, X., Lu, R. and Shen, X., 2014. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal*, *1*(5), pp.372-383.

[13] Hu, Y.C., Perrig, A. and Johnson, D.B., 2006. Wormhole attacks in wireless networks. *IEEE journal on selected areas in communications*, *24*(2), pp.370-380.
[14] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016

[15] Bogdanov, Andrey, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. "PRESENT: An ultra-lightweight block cipher." In *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 450-466. Springer Berlin Heidelberg, 2007.

[16] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 1996. *Handbook of applied cryptography*. CRC press.

[17] Touati, Lyes, Yacine Challal, and Abdelmadjid Bouabdallah. "C-cp-abe: Cooperative ciphertext policy attribute-based encryption for the internet of things." In Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, pp. 64-69. IEEE, 2014
[18] Beaulieu, Ray, Stefan Treatman-Clark, Douglas Shors, Bryan Weeks, Jason Smith, and Louis Wingers. "The SIMON and SPECK lightweight block ciphers." In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, pp. 1-6. IEEE, 2015

[19] Prasetyo, Kurniawan Nur, Yudha Purwanto, and Denny Darlis. "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA." In Information and Communication Technology (ICoICT), 2014 2nd International Conference on, pp. 75-79. IEEE, 2014

[20] Touati, Lyes, and Yacine Challal. "Efficient cp-abe attribute/key management for iot applications." In Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, pp. 343-350. IEEE, 2015

[21] Yao, Xuanxia, Zhi Chen, and Ye Tian. "A lightweight attribute-based encryption scheme for the Internet of Things." Future Generation Computer Systems 49 (2015): 104-112.

[22] Nawari, Mustafa, Hazim Ahmed, Aisha Hamid, and Mohamed Elkhidir. "Fpga based implementation of elliptic curve cryptography." In Computer Networks and Information Security (WSCNIS), 2015 World Symposium on, pp. 1-8. IEEE, 2015

[23] Touati, Lyes, and Yacine Challal. "Batch-Based CP-ABE with attribute revocation mechanism for the internet of things." In Computing, Networking and Communications (ICNC), 2015 International Conference on, pp. 1044- 1049. IEEE, 2015

[24] Yalçin, T., 2016. Compact ECDSA engine for IoT applications. *Electronics Letters*, *52*(15), pp.1310-1312.

[25] Touati, Lyes, and Yacine Challal. "Collaborative KPABE for cloud-based internet of things applications." In Communications (ICC), 2016 IEEE International Conference on, pp. 1-7. IEEE, 2016

[26] Oualha, Nouha, and Kim Thuat Nguyen. "Lightweight Attribute-Based Encryption for the Internet of Things." In Computer Communication and Networks (ICCCN), 2016 25th International Conference on, pp. 1-6. IEEE, 2016

[27] Mao, Y., Li, J., Chen, M.R., Liu, J., Xie, C. and Zhan, Y., 2016. Fully secure fuzzy identity-based encryption for secure IoT communications. *Computer Standards & Interfaces*, *44*, pp.117-121.

[28] Li, F., Zheng, Z. and Jin, C., 2016. Secure and efficient data transmission in the Internet of Things. *Telecommunication Systems*, *62*(1), pp.111-122.

[29] Tsai, K.L., Huang, Y.L., Leu, F.Y. and You, I., 2016. TTP Based High-Efficient Multi-Key Exchange Protocol. *IEEE Access*, *4*, pp.6261-6271.

[30] Adnan, S.F.S., Isa, M.A.M. and Hashim, H., 2016, May. Timing analysis of the lightweight AAβ encryption scheme on embedded Linux for Internet of Things. In *Computer Applications & Industrial Electronics (ISCAIE), 2016 IEEE Symposium on* (pp. 113-116). IEEE.

[31] Choi, Keun-Chang, and Moon-Seog Jun. "A Design of Key Agreement Scheme Between Lightweight Devices in IoT Environment." In *International Conference on Computer Science and its Applications*, pp. 224-229. Springer Singapore, 2016.