Security and Privacy Mechanism 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. Vivek Sehgal

By

Mukesh Sharma, Roll No. 152205

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

Certificate

This is to certify that synopsis report entitled **“Security and Privacy Mechanism in IoT”,** submitted by **Mr. Mukesh Sharma** 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: 2nd June.2017 **Dr. Vivek Sehgal**

Associate Professor

Department of Information Technology

JUIT Solan H.P.

Acknowledgement

I earnestly wish to express my heartfelt thanks and a sense of gratitude to my guide **"Dr. Vivek Sehgal"** Associate Professor, Information Technology Department, for his valuable guidance and constant inspiration in preparing this report. 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 wish to express my gratitude and high regards to **Dr. Pardeep Kumar** M. Tech Coordinator of CSE department, JUIT.

Last but not the least, I heartily appreciate all those people who have helped me directly or indirectly in making these task a success. In this context, I would like to thank all the other staff members, both teaching and non-teaching. My friends were always very helpful to me. They were always there for me whenever I needed their support.

Date: 2nd June.2017

Mukesh Sharma
152205

Table of Contents

Abbreviation and Symbols

IoT	Internet of thing
RFID	Radio-frequency identification
DTLS	Datagram Transport Layer Security
TLS	Transport Layer Security
LLN	Low-power and Lossy Network
E2E	End-to-End.
CoAP	Constrained Application Protocol
CN	Constrained Network
UCN	Unconstrained Network
M2M	Machine to Machine
CP-ABE	Cipher text-Policy Attribute-Based Encryption
ABE	Attribute-Based Encryption
KP-ABE	Key-Policy Attribute-Based Encryption
IBE-ECC	Identity Based Encryption- Elliptic Curve Cryptography
SRI	Socially Responsible Investing
NIST	National Institute of Standards and Technology
RBAC	Role Base Access Control
ABE	Attribute-Based Encryption
KP-ABE	Key-Policy Attribute-Based Encryption
CP-ABE	Cipher content Policy Attribute-Based Encryption
C-CP-ABE	Cooperative Cipher text Policy Attribute-based Encryption
FSFIBE	Fully secure fuzzy identity-based encryption

List of Figures

List of Table

Abstract

IoT is a new platform for connection smart devices in the network. It is domain where objects and people are associated, and they trade information over the connection using embedded sensors. The key thought of the Internet of Things is link embedded devices to everyday objects to make them shrewd devices. As large devices are connecting day by day into a network, huge amount of data is also generated. So the success of IoT is strongly depends upon the security and privacy. In this thesis we have discuss about the IoT security, also discuss the Security architecture of IoT which further categorized in two types i.e. off -line architecture and On-line architecture and listed various attacks in IoT which distort the normal functioning of the IoT architectures.

In the case of IoT there are various key challenges as compared to the traditional network model. So the traditional technique of security and privacy problems that were initially intended for the Internet will not function because these solutions require a huge quantity of resources and energy, which constrained devices most likely do not possess. So there is need to upgrade the implementations designs to cop up security and privacy challenges in the IoT.

In this thesis we have proposed a model for a scenario of country security from terrorist, trying to enter in the country from borders. Here we need to increase the security by establishing the Long Range Body Heat Detector with IoT devices. These sensors detect the human Body heat and pass the information to the IoT device which is connected with the sensor. In this scenario we have used the technique i.e. IBE-ECC which provide the security and privacy to the model because this approach use trusted third party called Private key Generator which generate private key and public key. This technique secures the information by using ECC and also provides privacy using central authority. This technique provides privacy, confidentially, availability, authentication, authorization, etc.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Kevin Ashton present the term Internet of Things in the year 1999 for supply chain management [1]. But now days it changing the world. As the measure of devices diminishing day by day. This interesting idea called Internet of Things imagining every one of the device or Things associated through the traditional network with the world. IoT is a domain where objects and people are associated, and they trade information over the connection using embedded sensors like cars, coolers, lights, Indoor regulators, Wearable gadgets [2] and more apparatuses associated with the IoT. It is evaluated that the quantity of IoT gadget associated in the system is more than 50 billion by 2020. The key thought of the Internet of Things is link embedded devices to everyday objects to make them shrewd devices [3]. These shrewd devices associated with the internet, will be exceptionally identifiable and furthermore ready to speak with each other and external world too. These devices require the capacity to Collect, Process and Transmit data. This is conceivable through the utilization and joining of existing technologies like Mobile technology, Smart sensor network, near field communication, Internet and so on by consolidating these technologies into the system.

IoT environment will be comprised of large heterogeneous devices. Because of the heterogeneous nature of the IoT environment, might be a few devices are constrained in nature. Constrained devices are devices that may shape systems which have low throughput and a high probability of packet loss. This is because constrained devices have limited processing bandwidth, memory, power capabilities [4]. That is the reason general answers for security and privacy issues that were initially intended for the Internet won't work in light of the fact that these solutions require a tremendous amount of resources and energy, which constrained devices probability don't have.

As per the SRI Counseling Business Knowledge, IoT will be create with integration of software and advanced sensors as appeared in the figure 1, this procedure can be isolated into 4 phases [5].

1) Supply-Chain Helpers based on RFID technology, it increment checking and sorting things to enhance co-ordinations speed and lessen misfortunes.
2) Vertical-Market Applications created for the enterprises to diminish working costs, for example, observing, transportation, medicinal services, security and other vertical applications.
3) Ubiquitous positioning it finds individuals and everyday objects in the region.
4) Physical World web, it remotely controls and senses far off items by methods for scaling down, less power utilization.

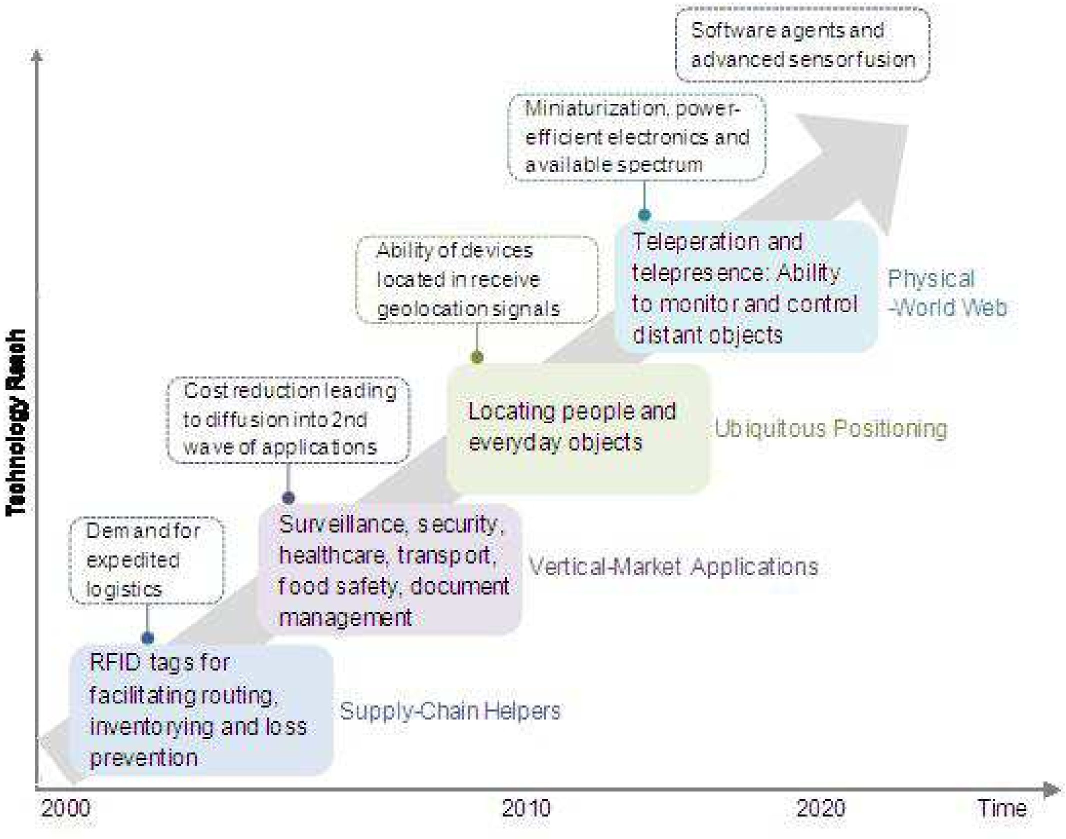

Software agents and advanced sensor fusion
Miniaturization, power-efficient electronics and available spectrum
Ability of devices located in receive geolocation signals
Teleperation and telepresence: Ability to monitor and control distant objects
Physical -World Web
Cost reduction leading to diffusion into 2nd wave of applications
Locating people and everyday objects
Ubiquitous Positioning
Technology Reach
Demand for expedited logistics
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
RFID tags for facilitating routing, inventorying and loss prevention
Supply-Chain Helpers
2000
2010
2020
Time

Figure 1.1 Technology roadmap: the Internet of Things [5]

1.1.1. Network Layers of IoT Architecture

There are many existing security technologies and arrangements can be oil in network architecture, particularly server farm cloud layers and over the core, there are diverse difficulties in the IoT space. The way of the end-points and the accelerate size of total require unique thought in the general engineering to hold these difficulties. The IoT architecture is made out of four layers; some are identified with those depicted in standard network architectures [6].

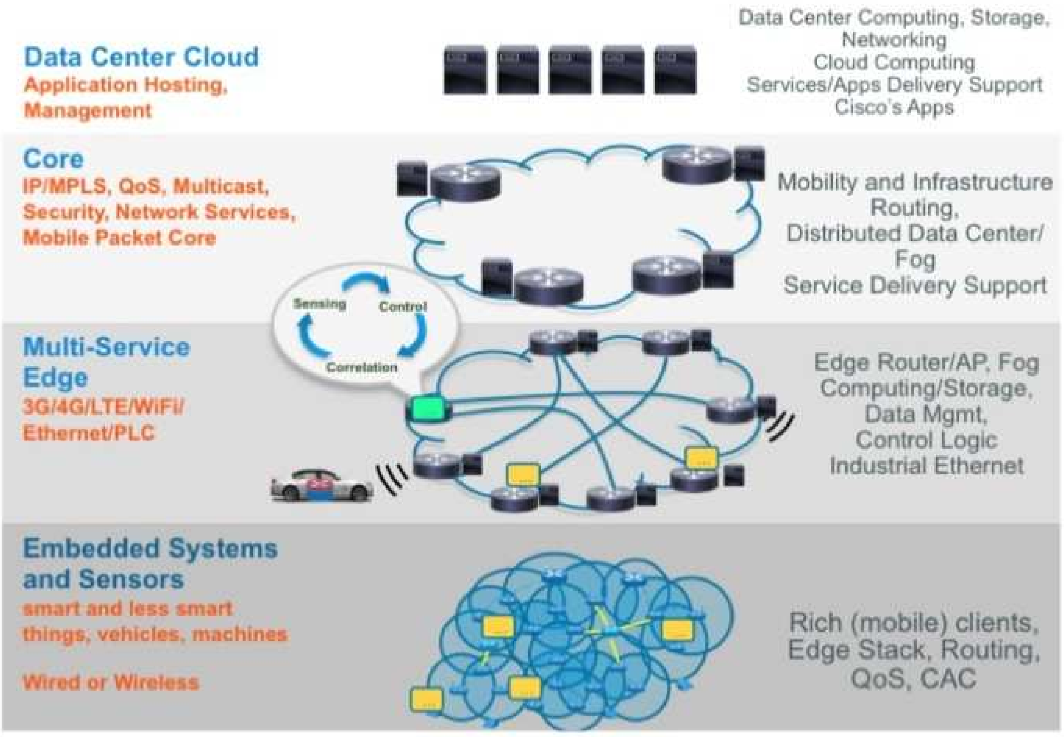

Data Center Cloud
Application Hosting, Management
Data Center Computing, Storage, Networking
Cloud Computing
Services/Apps Delivery Support
Cisco's Apps
Core
IP/MPLS, QoS, Multicast, Security, Network Services, Mobile Packet Core
Mobility and Infrastructure Routing,
Distributed Data Center/ Fog
Service Delivery Support
Sensing
Control
Correlation
Multi-Service Edge
3G/4G/LTE/WiFi/ Ethernet/PLC
Edge Router/AP, Fog Computing/Storage,
Data Mgmt,
Control Logic
Industrial Ethernet
Embedded Systems and Sensors
smart and less smart things, vehicles, machines
Wired or Wireless
Rich (mobile) clients,
Edge Stack, Routing,
QoS, CAC

Figure 1.2 IoT Network Architecture Layers by Cisco

A. Embedded Systems Layer

The main layer of the IoT configuration is containing embedded systems, sensors and actuators. These are small devices, with different working framework, memory, CPU type etc. An expansive part of these things are depended upon to be modest, single-function devices with direct framework accessibility, such as a weight or temperature sensor [6]. These devices could be in remote or out of reach territories where human hindrance or setup is for all intents and purposes inconceivable.

Since the method for sensors is to such a degree, to the point that they are embedded in what they are recognizing none can picture another workplace, school improvement wander or recuperating focus where these sensors are familiar in the midst of the advancement arrange with collect and monitor information and facts. Strategies must be taken to ensure the authenticity of data, path from the sensor to the collect and system between the basic foundations of the devices.

B. Multi-Service Edge Layer

The capriciousness in the limits of end-point gadgets, and their conceivably over the top numbers highlight the complement of the multi-service edge in the IoT architecture. The multi-service edge is multi-module based both wireless and wired network. In fact, even inside those two orders, this layer must bolster various distinctive traditions, such as 3G and 4G, to contain a Varity of end-core interests. The traditions used by these devices might not have any certain security capacities. It is basic for security administrations to guarantee these inalienable uncertain endpoints.[6] This layer must be standard to scale to meet development requirements. The segments and administrations offered inside one module ought to be near so that additional modules can be incorporated a constrained capacity to center time.

C. Core Network Layer

The design of the core network layer is identified with the architecture utilized as a part of conventional network. This layer gives ways to trade and convey information and system data between various sub-systems. The principle distinction among IoT and customary center layers is traffic profile. The IoT information and activity might be distinctive. Security administrations at the core network guarantee that the IoT framework all in all, and have been prepared to ensure against dangers like eavesdropping, spoofing, reply attack etc.

D. Data Center /Cloud Layer

The architecture of the data center/cloud network layer is likewise like the architectures that are utilized as a part of customary networks. This layer oversee applications that are giving administrations and to deal with the end-to-end IoT architecture. Likewise, security benefits in the data center/cloud system are basic in guaranteeing that the IoT framework all in all has been solidified to ensure against threats like transaction replays, Denial of Service and so on.

1.2 Problem Statement

With the proliferation of IoT devices, the integration of these devices into the standard Internet introduces several security and privacy challenges. As IoT devices are constrained devices, they have less resources like memory, processing and power as compare to the traditional deices. That's why universal solutions to security and privacy problems that were initially intended for the Internet will not function because these solutions require a huge quantity of resources and energy, which constrained devices most likely do not possess. So there is need to upgrade the implementations designs to cop up security and privacy challenges in the IoT.

The fields of network administration, correspondences, figuring, communications, computing, process, equipment and programming have change the method for individuals, shrewd items, system connect and exchange data. The Internet of Things will fuel the accomplishment of this new interconnected world. This system unequivocally depends upon the security and protection of Internet of Things, and in addition the sensitive information winded [4]. In spite of the fact that these innovations additionally offer numerous abilities like the development of equipment and programming many-sided quality, and also the presence of worldwide get to, increment the weakness to security attacks.

1.3 Objectives

The aim of the thesis is to provide the security and privacy to the IoT devices. Because the success of IoT is depends on the security and privacy only. In this thesis a scenario is of county security has been taken to secure the country boarders from the terrorist. So this application required more security and privacy. This thesis contain security model to protect the communication between the IoT devices and the master node. This model also protects the IoT privacy information. The criteria of the designs are as follow:

1) Security
2) Resilience to attacks
3) Authentication
4) Privacy protection
5) Low cost

1.4 Outline

The structure of this thesis is as follows. Chapter 2 presents relevant background information about Information Security and privacy in IoT. Chapter 3 presents the detailed information Security in IoT, like issues, characteristic, various attacks, and cryptographic techniques. Chapter 4 presents information about the privacy in the IoT. Chapter 5 presents the methodology and proposed approaches to overcome the security and privacy in IoT. Chapter 6 presents the results and analysis of our proposed model. Chapter 7 draws the conclusion of the thesis and future work.

CHAPTER 2

LITERATURE SURVEY

2.1 Literature Survey

Compact smart devices create a main part of Internet of Things. The integration of these smart things into the normal Internet introduces several security, privacy and trust challenges because the majority of Internet technologies were not designed to support IoT. And also the success of these devices fully depends on the security and privacy of IoT. In this section, give an introduction to the venerability and survey of the challenges in IoT.

Nia, A. M. et al. in [6] Explore and address the threats which can leads to exploit the IoT. And also introduce two emerging security challenges that can be exploited by the attacker are Exponential increase in the number of weak links and Unexpected uses of data.

Brachmann et al. in [7] The security conventions like TLS or DTLS fruitful in Internet yet it doesn't imply that same security level can be accomplished in the event of interconnecting the internet with the Low-power and Lossy Network. E2E security in IoT is not unimportant, on account of numerous conceivable use situations like: CoAP/CoAP, DTLS/DTLS and HTTP/CoAP, TLS/DTLS interceded by a 6LBR that have diverse requirements and limitations. They additionally concede that having a safe E2E association between two end has just keep a protected correspondence channel, the LLN can even now be vulnerable against asset utilization, flooding, replay and amplification assaults, since the 6LBR ordinarily does not accomplish any validation.

Bonetto et al. in [8] they outline the utilization cases and down to earth cases relating to secure communications catching into record the convention stack design. Also, propose a lightweight technique to fabricate a end-to-end secure channel, requiring negligible inclusion of constrained IoT gadgets, while keeping all convention operations unaltered inside the UCN. This is accomplished through the change of a portion of the means consolidated with channel foundation to a trusted in Gateway.

Al Alkeem et al. in [9] they propose three different security levels depending on the sensors location on the wearable system. Patients use a wearable device which measures body activities and converts the body signals to values in order to be understood by a human. Such information is reflected in classification matrix. The information which is classified as restricted, can apply intermediate security level such as mutual authentication and exact location of patients. The authentication part can be achieved using a PIN code with a biometric token. A successful authentication, role base access control (RBAC) can be considered in which permissions are combined with roles, and users made members of certain roles for patients' data records.

Harris et al. in [10] This paper displayed Lamina, a versatile framework that setup protection and security for client gadget cooperation in broad daylight IoT spaces. It incorporates an out-of-band, cloud based enlistment framework where keying material is traded between the client gadget and the coveted open IoT space. Once the keying material is traded, Crypto CoP-based encryption and MAC address cycling are utilized on the client gadget to secure outsiders can't get private data about the client that is imparted to the IoT space. Lamina additionally ensure the general population IoT space can gather enough recognizing data in regards to clients traversing the space to give Targeted data and administrations while as yet securing the client's identities.

Chen et al. in [11] There is an immense interest for security arrangements. Hence, the proposed SGA could give a shared confirmation component, and maintain a strategic distance from the key speculating assault, the imperceptible on-line key speculating assault, the information security and hand-off assault. The SGA proposed in this paper meets the center security prerequisites of the Machine to Machine service layer. To guarantee each shrewd gadget can safely speak with each other, the security passage application incorporates the Lightweight Symmetric Key Cryptographic assertion Function, Secure End-to-End and Machine-to-machine Key Exchange.

Arseni et al. in [12] The proposed architecture design tries to finish existing testing stages and to enable developers to have a superior outline of what is the execution of their calculations on a few sorts of stages, with the goal that they can make changes in accordance with get the most elevated amount of security that the algorithm can guarantee. Additionally, the tried permits the testing of algorithm coordinated straightforwardly in hardware, while having the likelihood for parallel testing on the staying base architectures.

Olivier et al. in [13] they gave another design various programming software-defined networking controllers in equivalent cooperation. Likewise proposed a design which is versatile with different SDN domain. In every space, systems with or without structure and every controller is responsible just for its domain. The communications between domain is made with fitting controllers called Border Controllers. In the event of disappointment these edge controllers need to work in another circulated connection keeping in mind the end goal to ensure the autonomy of every domain. They select architecture which ensures the security of the whole system with the idea of lattice of security implanted in every controller to anticipate assaults.

Evans et al. in [14] In this paper an information labeling for overseeing privacy in IoT is proposed. This method taken from the information characterizing, Information Flow Control organize occasions can be labeled with various privacy property such labels enable the framework to reason about the claims of information and ensure the privacy of people. Misusing labeling inside obliged sensor hubs may not be an appropriate arrangement by reason of labels might be excessively immense with deference, making it impossible to the information size and sensitivity, in this way they create an intemperate overhead. For this situation it is not appropriate for IoT.

Wang et al. in [15] In this paper dissects the lead of the two noteworthy sorts of Attribute-Based Encryption (ABE): Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher content Policy Attribute-Based Encryption (CP-ABE). Simulations are carried on deferent classes of cell phones, including a portable workstation and an advanced cell, so as to build up under what conditions ABE is more qualified for IoT. ABE gives an public key encryption conspire which empowers a grained get to control, a versatile key administration, and information appropriation.

Schurgot et al. in [16] they have given an underlying investigation of the risks to security and protection of IoT systems, concentrating on home computerization systems. There studies have concentrated essentially on privacy safeguarding. Protecting privacy is critical to accomplishing the capability of billions of associated devices and examination, for example, giving savvy home advances to spare vitality and enhance home security. They give an outline to modest investigation of IoT security and protection utilizing COTS items and services. These cheap test-beds can give understanding into other IoT applications. They show that both straightforward cryptographic systems and data control can be utilized to ensure a client against an enemy inside the IoT arrange or a foe that has traded off remote servers. They demonstrate the utility of proxying IoT arrange information through VPN overlay systems. This can turn into a non specific support of IoT clients, closely resembling Web perusing secrecy given by Tor.

Touati et al. in [17] In this paper they have proposed a batch-based rendition for Cipher content Policy Attribute-Based Encryption to accomplish traits denial in an Internet of Things condition. Their Solution diminishes the overhead and the many-sided quality, and it doesn't require re-scrambling information each characteristic approach change.

Bogdanov et al.in [18] “PRESENT: An Ultra-Lightweight Block Cipher” Author present a ultra-lightweight block cipher that is suitable encryption technique for resource constrained devices. A present block cipher is based on SP network **[19].**Present block cipher provided hardware efficiency. But used when application required moderate security levels. The main drawback of this paper is it is implemented in hardware and Moderate security levels.

Lyes Touati et al .in [20] “Cooperative Cipher text Policy Attribute-based Encryption For the Internet of Things ” Author present a cooperative cipher text policy attribute based encryption technique as an alternative solutions to protecting data when data transfer over public network from IoT end nodes. Deed the heterogeneous nature of the IoT to make viable the use of the CP-ABE scheme in an IoT domain, transfer the task from highly resource-constrained devices to unconstrained one by hand over heavy operations in CP-ABE scheme to neighbor un constrained nodes. The main idea behind C-CP-ABE is to disburse computation of CP-ABE encryption primitive ,the resource–constrained object can hand over the most consuming operations to unconstrained nodes of the network. The computations of CP-ABE encryptions primitive is transpose from resource-constrained devices to unconstrained ones. This technique required trusted unconstrained nodes in its neighborhood.

Ray Beaulieu et al. in [21] “The SIMON and SPECK lightweight block ciphers” Author present 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. But implemented in hardware.

Kurniawan Nur Prasetyo ST et al.in [22] “An Implementation of Data Encryption for Internet of Things Using BLOWFISH ALORITHM on FPGA” Author present a blowfish algorithm is implemented on FPGA using VHDL programming language. Using FPGA implementation is cheap, easy to implement, reprogrammed and high speed. Reduce total encryption time, give greater throughput and not affect avalanche effect significantly. But this technique is costly and required hardware.

Lyes Touati et al .in [23] “Efficient CP-ABE/Key Management for IoT Applications” proposed a solution does not involve suspension ensuing access grants and revocations. Omit the overhead as a result of to re-encryption and renaming attributes and does not compulsory proxies to achieve attribute revocations , dwindle to the minimal number of chunk generated private key and does not actuate any delay. The author proposed a Solution with actuates zero delay and a minimal of generated secret key parts. The main idea behind this solution is to divide time axis into time slots with variable period, Trusted Attribute Authority has not to rename attributes in order to revoke them from some users ,and has not also to regenerate all private key for all users every attribute revocation ,it generates only chunk of the private key relevant to an attribute.

Xuanxia Yao et al. in [24], “A lightweight attribute-based encryption scheme for the Internet of things” proposed a light weight no-pairing ABE technique based on elliptic curve cryptograph. The security of this technique is based on ECDDH posit rather than bilinear Diffie-Hellman posit , which can curtail the data processing overhead and communication overhead.ABE technique layout just for one authority applications, it is not pertinent to Ubiquitous IoT applications.

Mustafa Nawari et al. in [25] “FPGA based Implementation of elliptic curve cryptography” proposed a elliptic curve cryptosystem mellow by programming Spartan3E FPGA kit and analyzed by implementing Elgamla encryption plan on it. It contribute the same level of the security that other surrogate contribute, it performs processing in less time, less memory, less computations and less power consumption. It is pertinent for resource constrained devices in the IoT. Hardware implementation of elliptic curve cryptography using FPGA boost the system performance and a lot of protected than software implementation. But this technique is costly and required hardware.

Lyes Touati et al.in [26] “Batch-BASED CP-ABE with Attribute Revocations Mechanism for the IoT” present a new technique to reduces the complexity and the overhead, and does not required extra trust nodes in the system. In batch –based mechanism that time axis is divide into intervals of the same duration that is called time slots, policy access changes occur only between two successive time slots. Trust node assign only the vital attribute key chunks every time slot to grant a thing to update its private key. Procedure has need synchronization between all things in system. It does not compulsory to re-encrypt data every attribute policy change. Batch-Based CP-ABE with Attribute Revocations Mechanism using time slots idea. But this technology needs synchronization of nodes.

T. Yalçin et al .in [27] “Compact ECDSA engine for IoT applications “proposed ECDSA for encryption and decryption process in IoT using elliptic curve and digital signature algorithm. ECDAS engine is implemented as an intellectual property (IP) in a 180 nm processes this hardware encryption and decryption technique. But this technology is costly and Suitable for Hardware Implementation.

Lyes Touati et al.in[28]“Collaborative KP-ABE for Cloud-Based Internet of Things Applications “Author proposed KP-ABE scheme using the computing power and storage capacities of cloud server and trust node for doing computations. The main advantage is it have heavy operations of the encryption process to trusted unconstrained assistant nodes and a cloud server. But each resource constrained device there are at least two trusted unconstrained devices in its neighborhood.

Nouha Oualha et al. in [29] “Lightweight Attribute-based Encryption for the Internet of Things” proposed CP-ABE schema using effective pre-computation techniques. The key concept behind pre-computation techniques is to pre-compute and cache a set pairs collected with commonly exorbitant cryptographic operations. Pre-computation techniques based on the generator, the preprocessing algorithms of the generator are execute by the hardware devices or trusted authority. Pre-computation technique reduce the cost of CP-ABE encryption, pre-computation technique used less computation and less energy drain than original schema**.** But this technique require more storage space.

Yijun Moa et al. in [30], “Fully secure fuzzy identity-based encryption” proposed a new FSFIBE technique to protecting data transmission in IoT. FSFIBE technique is secure in the full model without random oracles. FSFIBE technique has tight security reduction and constant size of public parameters O (1).FSFIBE technique provided property of error-tolerance. It is more pertinent for protecting IoT communications. But Enlarge Key size for encryption and decryption.

Fagen Li et al.in[31] “Secure and efficient data transmission in the Internet of Things “Author propose a heterogeneous ring signcryption technique for secure communication form recourse constrained devices to server over a public network. The heterogeneous ring signcryption technique avow sender in IBC environment to send a message to a receiver in the PKI domain. The technique at the same time obtains confidentiality, integrity, authentication, non-repudiation and anonymity in a sensible single step.

Kun-Lin Tsai et al. in [32] “TTP based High-efficient Multi-Key Exchange Protocol” Author proposed third party based multi key exchange protocol and use elliptic curve encryption and decryption. Secure against five attacks (Replay attack, Eavesdropping attack, Known-key attack, Impersonation attack, Forgery attack). But increase overhead in third party.

Syed Farid Syed Adnan et al .in [33] “Timing Analysis of the Lightweight AAβ Encryption Scheme on Embedded Linux for Internet of Things “Author present an analysis of lightweight asymmetric encryption, the AAβ (AA-Beta) .that may be feasibly in IoT. 99% improvement on encryption time and improvement of 94% on decryption time for 2048-bit primes. This technique is suitable for some applications only.

Keun-Chang et al .in [34] “A Design of Key Agreement Scheme between Lightweight Devices in IoT Environment”. Author proposed a protocol for low power and low speciation devices communicate using user smart devices through gateway and certificate authority. This protocol provides protection form re-use attack and middle attack.

CHAPTER 3

SECURITY

The team Data Security for procedures and philosophies used to ensure data, information and system. With respect to Information Security, ensuring mean averting unauthorized access, use, disturbance, disclosure, modification or destruction. Data Security has three key rules that can be thought about. These are confidentiality, availability, integrity [50] [51]. Accountability has turned out to be more critical standard and is some of the time included among the three ideas by security organizations for example Combitech AB and so on.

3.1 IoT Security Concepts

The protection allow to an information system in order to secure the relevant objectives of retain the availability, integrity, and confidentiality of information system resources. **[52]**

There are some key objectives for securing IoT devices in the network.

- **Confidentiality:** Defending authorized limitations on data get to and spill, including implies for securing individual protection data. Lost confidentiality is the unauthorized revelation of data.
- **Integrity:** Preserving despicable data alteration or misfortune, including guaranteeing data non-renouncement and authenticity. Lost integrity is the unauthorized modification or loss of data.
- **Availability:** Ensuring auspicious and solid get to and utilization of data. Lost availability is the intrusion of access to or utilization of data.
- **Authenticity:** The property of being bona fide and having the capacity to be trusted and checked affirmation in the validity of a transmission, a message. This

implies verifying that clients are who they say they are and that each input arriving at the framework originated from a trusted source.

- **Accountability:** The security objective that produces the requirement for activities of an entity to be followed interestingly to that entity. This backings non-repudiation, deterrence, intrusion detection and prevention, fault isolation, and after-action recovery and legal action. Since really secure system is not yet a feasible objective, it must have the capacity to follow a security break to a responsible party.[52]

3.2 Security Architecture of IoT

This postulation will partition the IoT security architecture into two sorts, the off-line architecture and the on-line architecture. The off-line architecture is utilized as a part of the IoT application which is primarily made out of customary gadgets. The on-line architecture is connected to the IoT application which is primarily made out of shrewd gadgets. As indicated by the attributes of the two classes, this proposition will outline diverse answers for them.

3.2.1 Off-line IoT architecture

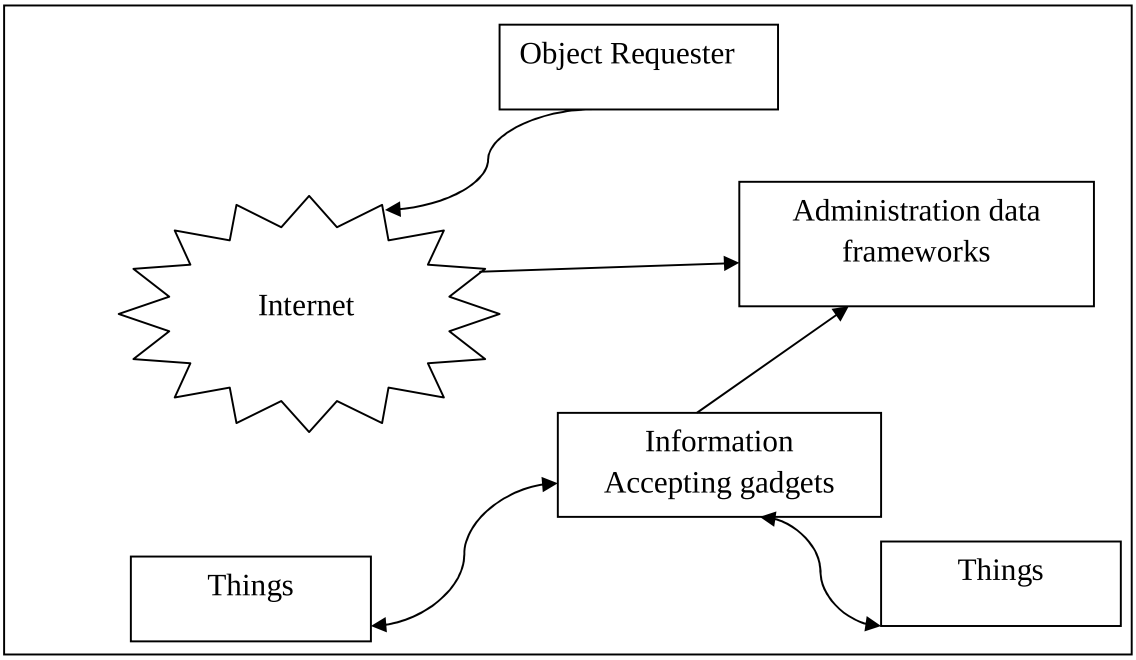


Figure-3.1 Off-line architecture for IoT

Figure 3.2.1 demonstrates that in the off line IoT design, the Things (recognition gadgets) just impart and trade information with data accepting gadgets. The validation and key understanding in off line design are separated into two sections: one is the validation and key understanding between the things and the accepting gadgets; the other is between the get to requesters and the administration data frameworks. The information seen by things incorporates in the administration data framework by the data getting gadgets. Get to requesters just interface with administration data frameworks to oversee, dissect and apply the recognition information. EPCglobal is a run of the mill off line architecture application.

As far as the things, there are no huge contrasts in the behavioral designs between the IoT and customary Internet applications. So the conventional security innovation can keep on being connected, for example, secret word based validation, certificate based confirmation and other normal verification, part based get to control display as well. With respect to the items, the verification and information correspondence security between them also, the accepting gadget will, from one perspective, influence the precision of the information investigation in ensuing IoT applications; then again, raising new necessities about security of protection.

3.2.2 On-line IoT architecture

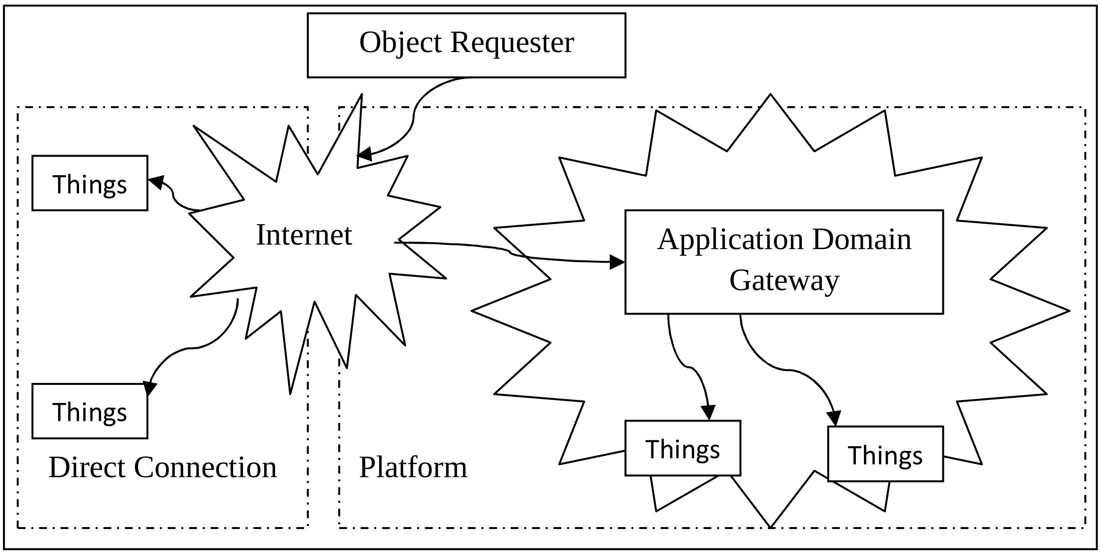


Figure 3.2 On-line IoT architecture

Figure 3.2.2 demonstrates that in the on-line IoT architectures, the things can set up end-to end correspondence connections to get to requesters by means of the Internet or IoT passage. The on-line architectures can be partitioned into direct association and stage two sub architectures.

In the immediate association IoT applications, get to requesters and things utilize the system to specifically associate. The things autonomously finish the access requester validation; get to control and other security assurances.

In the stage IoT applications, access requesters and things have a place with various security domain: get to requesters are in general public domain, and the things in the application area. The information correspondence between the two sides is continuing through the application domain gateway. The access requesters and the things don't set up coordinate system associations. The application domain gateway can finish the get to requester verification and get to control in various layers.

Since the stage IoT design applications build up the end-to-end correspondence connects amongst things and get to requesters, the usage procedure requires a great deal of accessible things name. Additionally, so as to encourage the examination of things tending to security in later parts, the things scale and question name asset of two sorts IoT architecture applications are looked at.

3.3 Security Challenges in IoT

There are many security challenges in IoT system as compare to the traditional model. The following lists some security challenges in designing and building IoT devices:

- Small in size, minimal effort gadget with next to zero physical security.
- Constrained in memory and figure assets, not ready to bolster mind boggling and widespread security algorithms on account of these components:
    - Limited calculation capacities
    - Encryption calculations require higher calculation asset and high power
    - Low CPU cycles for powerful encryption

- Designed to work independently in the field with no reinforcement network, if connection is lost.
- Scalability and administration of billions of entities in the IoT.
- Identification of end-focuses in a versatile way is an extraordinary test like
    - Individual
    - Group
    - In a few cases location might be more imperative than the individual identifier.

3.4 Characteristics of the Internet of Things

Characteristics	**Description**
Interconnectivity	Everything can be connected to the global information and communication infrastructure
Things-related services	Provides things-related services within the constraints of things, such as privacy and semantic consistency between physical and virtual thing.
Heterogeneity	Devices within IoT have different hardware and use different networks but they can still interact with other devices through different networks.
Dynamic changes	The state of a device can change dynamically, thus the number of devices can vary. (Device states: connected, disconnected, waking up, and sleeping)
Enormous scale	The number of devices operating and communicating will be larger than the number of devices in the current Internet. Most of this communication will be device to device instead of human to device.

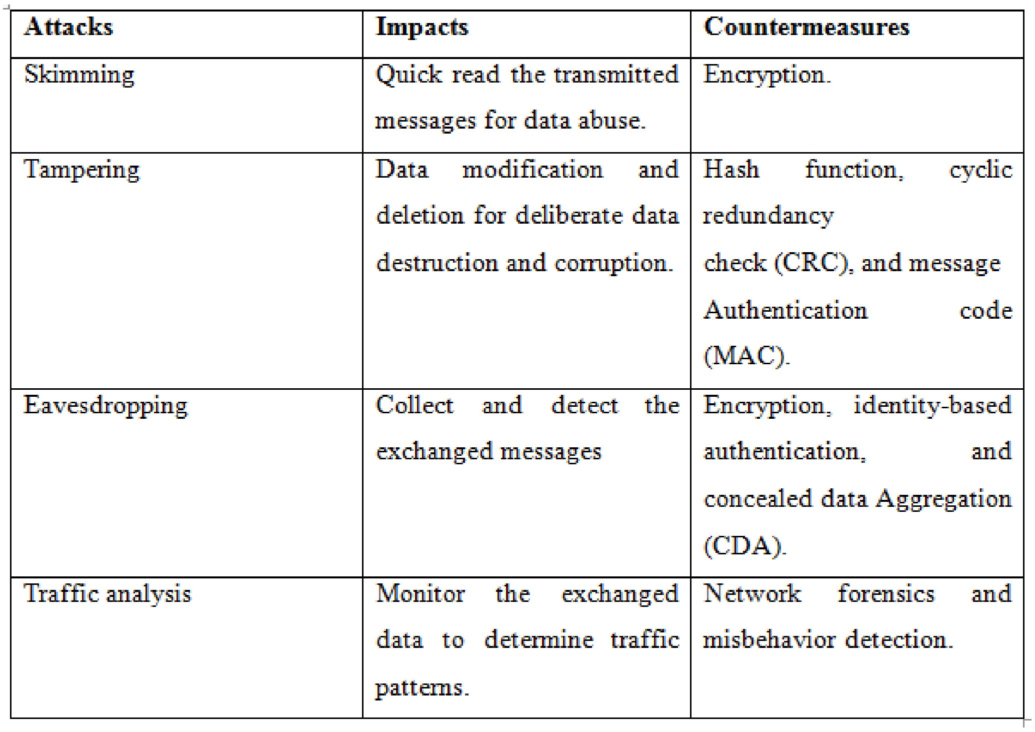
Table 3.1 Characteristics of the Internet of Things

3.5 Why IoT Security is Necessary?

IoT security is the way toward preventing and recognizing unauthorized utilization of device. Prevention action measures help us to stop unauthorized clients for getting to any piece of your IoT framework. Detection helps us to watch that somebody endeavored to break into your IoT framework, on the off chance that they were effective, and what they may have done with the IoT framework.

3.6 Various Attack on IoT network

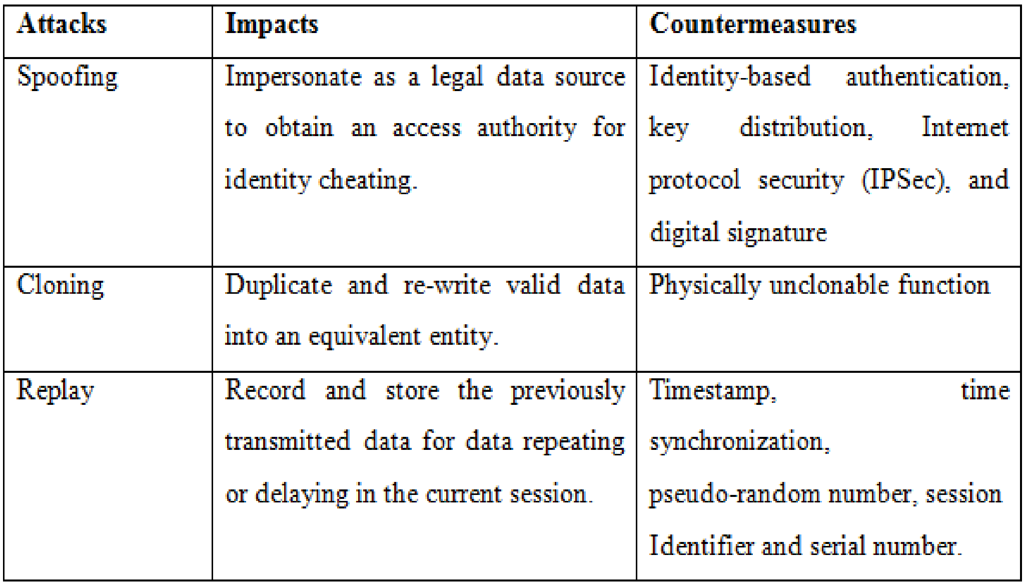
1. Information gathering attacks



Attacks	Impacts	Countermeasures
Skimming	Quick read the transmitted messages for data abuse.	Encryption.
Tampering	Data modification and deletion for deliberate data destruction and corruption.	Hash function, cyclic redundancy check (CRC), and message Authentication code (MAC).
Eavesdropping	Collect and detect the exchanged messages	Encryption, identity-based authentication, and concealed data Aggregation (CDA).
Traffic analysis	Monitor the exchanged data to determine traffic patterns.	Network forensics and misbehavior detection.

Table 3.2 Information gathering attacks

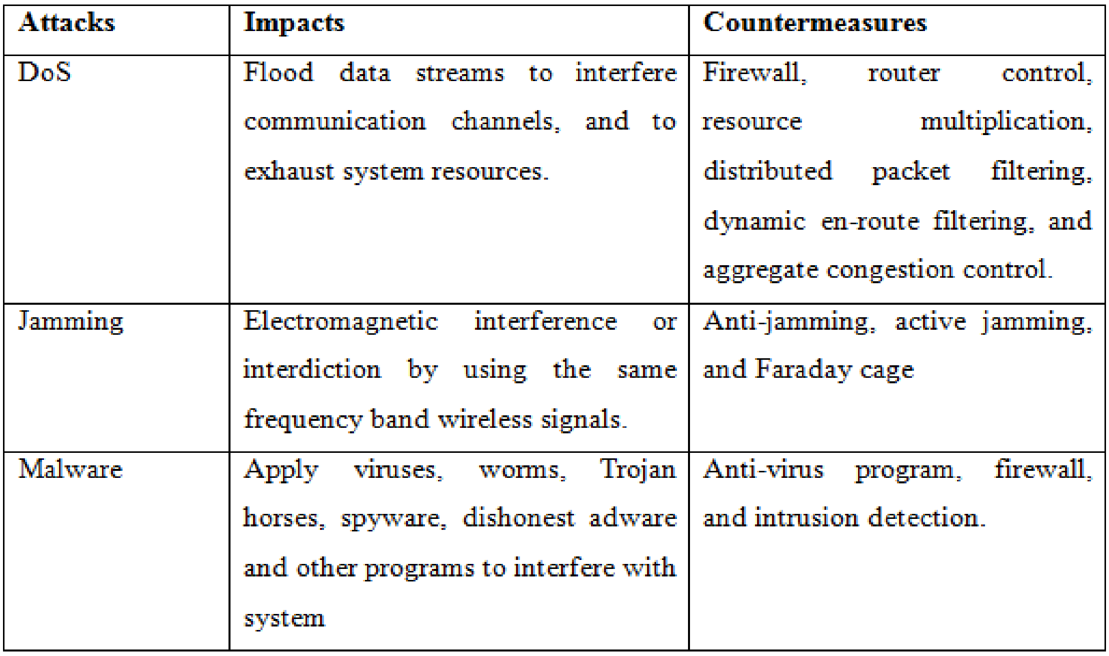
2. Information Imitation attacks



Attacks	Impacts	Countermeasures
Spoofing	Impersonate as a legal data source to obtain an access authority for identity cheating.	Identity-based authentication, key distribution, Internet protocol security (IPSec), and digital signature
Cloning	Duplicate and re-write valid data into an equivalent entity.	Physically unclonable function
Replay	Record and store the previously transmitted data for data repeating or delaying in the current session.	Timestamp, time synchronization, pseudo-random number, session Identifier and serial number.

Table 3.3 Information Imitation attacks

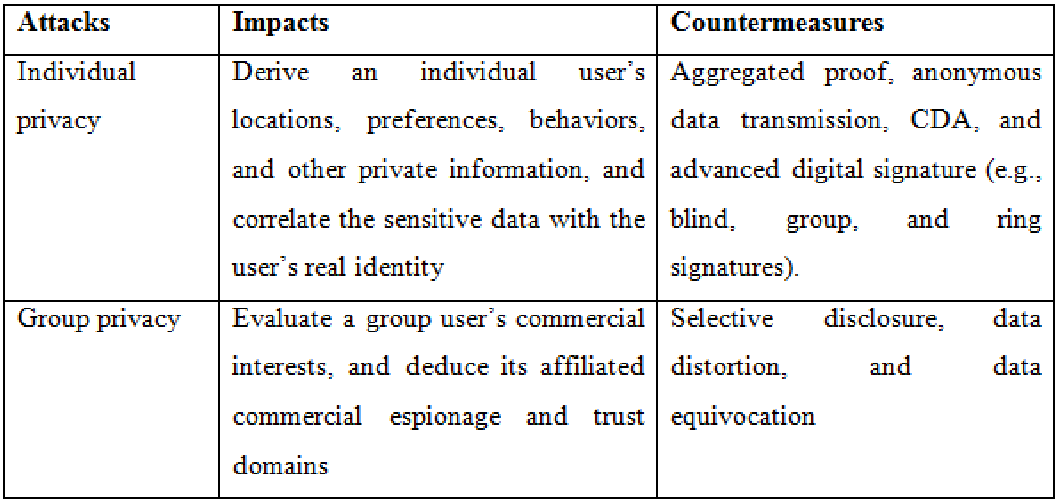
3. Channel blocking attacks



Attacks	Impacts	Countermeasures
DoS	Flood data streams to interfere communication channels, and to exhaust system resources.	Firewall, router control, resource multiplication, distributed packet filtering, dynamic en-route filtering, and aggregate congestion control.
Jamming	Electromagnetic interference or interdiction by using the same frequency band wireless signals.	Anti-jamming, active jamming, and Faraday cage
Malware	Apply viruses, worms, Trojan horses, spyware, dishonest adware and other programs to interfere with system	Anti-virus program, firewall, and intrusion detection.

Table 3.4 Channel blocking attacks

4. Attack on Privacy



Attacks	Impacts	Countermeasures
Individual privacy	Derive an individual user's locations, preferences, behaviors, and other private information, and correlate the sensitive data with the user's real identity	Aggregated proof, anonymous data transmission, CDA, and advanced digital signature (e.g., blind, group, and ring signatures).
Group privacy	Evaluate a group user's commercial interests, and deduce its affiliated commercial espionage and trust domains	Selective disclosure, data distortion, and data equivocation

Table 3.5 Attack on Privacy

3.7 What is Cryptography?

The interpretation of information into a mystery code. Encryption is the best approach to accomplish information security. To read an encoded document, you should have access to a mystery key or secret key that empowers you to unscramble or decrypt it. Plain text is called unencrypted data and cipher text is called encrypted. In other words, process of protection data from undesirable attacks by changing it in non-recognizable by attacker is known as Encryption. Information encryption for the most part is the scrambling of the content of information so forth to make the information unreadable, invisible or during transmission. The objective is to secure the content of the information against the attackers. The reverse of information encryption is information decryption, which recovers the original information [35].

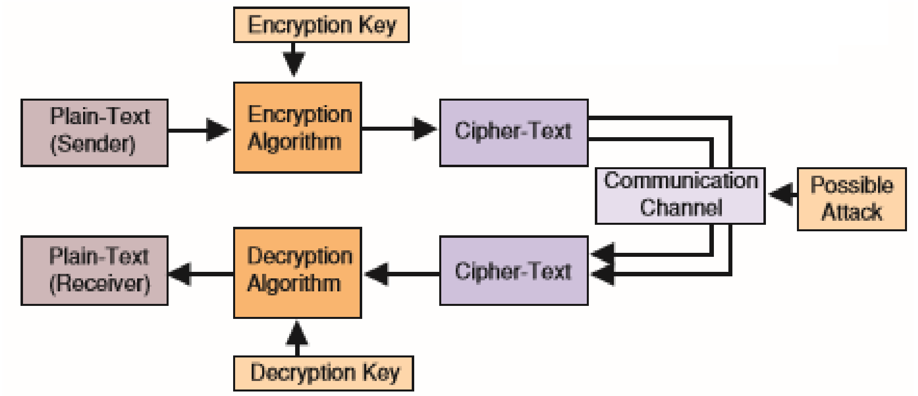


Figure 3.3- Encryption/decryption system [35]

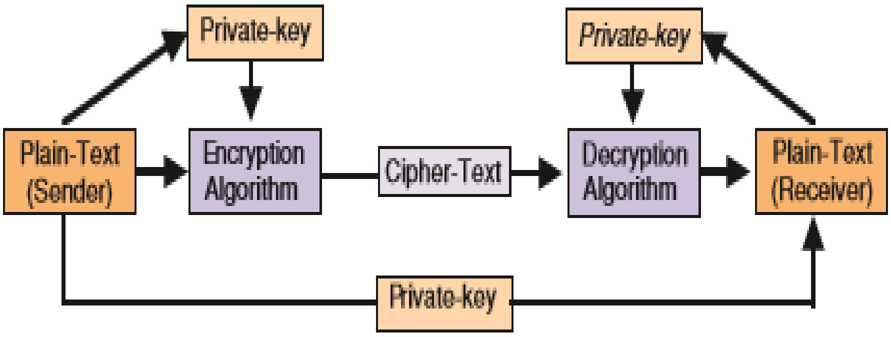


Figure 3.4- Private-key system [35]

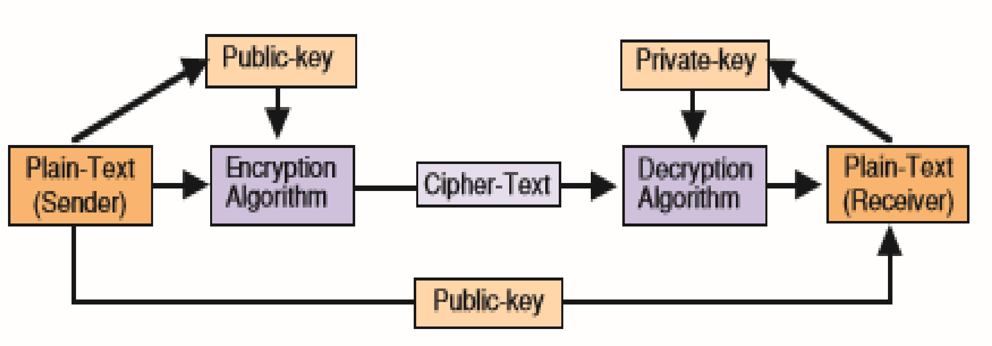


Figure 3.5- Public-key system [35]

3.8 Lightweight cryptography for IoT

Lightweight Cryptography is used in the IoT because of two reasons.

1. **Efficiency of end-to-end communication**

   To accomplish E2E security, end hubs have an implementation of a symmetric key algorithm. For the low resource-devices, e.g. battery-fueled devices, the cryptographic operation with a constrained measure of energy utilization is important. Use of the lightweight symmetric key algorithm permits brings lower energy utilization for end devices [36].

2. **Applicability to lower resource devices**

   The impression of the lightweight cryptographic primitives is smaller than the traditional cryptographic ones. The lightweight cryptographic primitives would open potential outcomes of more system associations with requirement gadgets or constraint devices. An examination of the lightweight properties with the general cryptographic primitives [36].

3.8.1 Type's Lightweight cryptography

1. Symmetric Key.
2. Asymmetric Key.

Symmetric Key

Symmetric encryption, additionally alluded to as traditional encryption or single key encryption was the main sort of encryption being used preceding the improvement of public key encryption.

The symmetric encryption has five steps.

1. **Plaintext:** This is the first clear message or information that is nourished to the algorithm as information.

2. **Encryption algorithm:** The encryption algorithm performs different substitutions on the plain text to convert it in cipher text or in unreadable form.
3. **Secret Key:** The Secret Key is likewise contribution to the encryption algorithm. The correct substitutions and changes performed rely on upon the key utilized, and the algorithm will deliver an alternate yield contingent upon the particular key being utilized at the time.
4. **Cipher text:** This is the mixed message created as yield. It depends on the plaintext and the Secret key. The cipher text is an evidently arbitrary stream of information, the way things are, is garbled.
5. **Decryption Algorithm:** This is an encryption algorithm that converts cipher text in to plain text with the help of secret key.

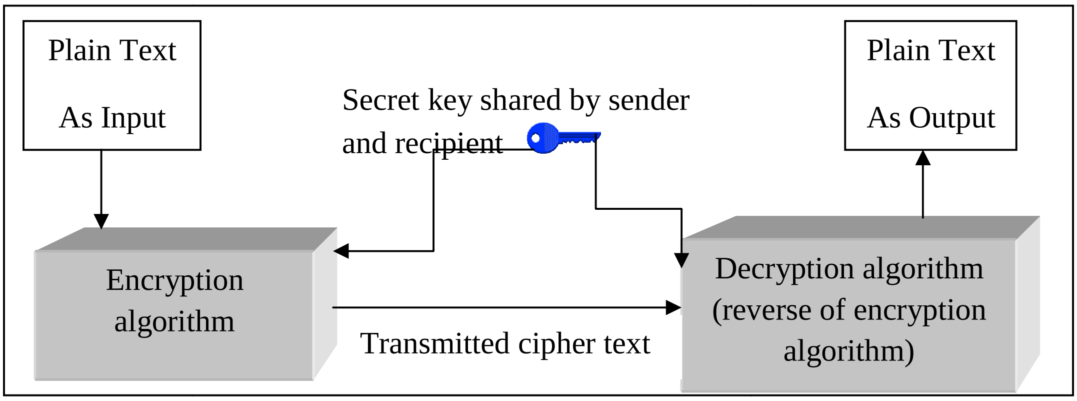

Plain Text
As Input
Secret key shared by sender and recipient
Plain Text
As Output
Encryption algorithm
Transmitted cipher text
Decryption algorithm (reverse of encryption algorithm)

Figure 3.6 Symmetric Encryption Model

Advanced Encryption Standard

AES expresses that the algorithm can just acknowledge a block size of 128 bits and a decision of 3 keys - 128, 192, 256 bits. Contingent upon which variant is utilized, the name of the standard is changed to AES-128, AES-192 or AES-256 individually. And these distinctions AES contrasts from DES in that it is not a feistel structure. Review that in a feistel structure, half of the information piece is utilized to change the other portion of the information square and after that the parts are swapped. For this situation the whole information square is prepared in parallel amid each round utilizing substitutions and changes [37].

Various AES parameters rely on upon the key length. For instance, if the key size utilized is 128 then the quantity of rounds is 10 though it is 12 and 14 for 192 and 256 bits individually. At present the most widely recognized key size liable to be utilized is the 128 piece key. This depiction of the AES algorithm along these lines portrays this specific usage [37].

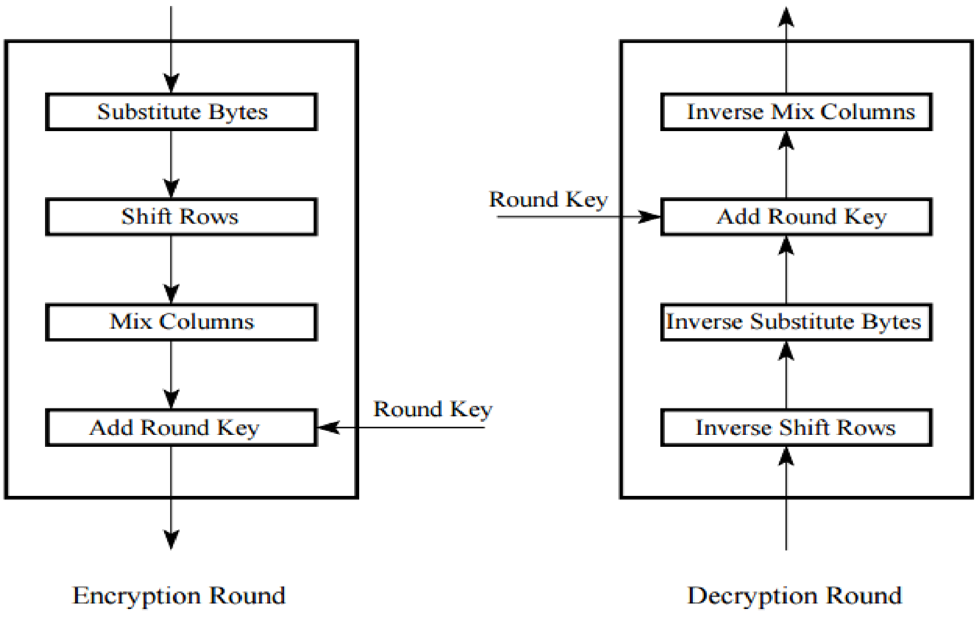


Figure 3.7 AES Encryption and Decryption [37].

RSA

This Algorithm depends on the trouble of factorizing substantial numbers that have 2 and just 2 components (Prime numbers) [38]. The framework deals with an open also, private key framework. General society key is made accessible to everybody. With this key a client can scramble information yet can't unscramble it, the main individual who can unscramble the one has the private key. It is hypothetically conceivable yet to a great degree hard to create the private key from general society key, this makes the RSA calculation an extremely well known decision in information encryption [38].

ECC

Elliptic Curve Cryptography (ECC) is a cryptographic idea in view of elliptic bends. By utilizing point duplication on focuses on a bend and using the elliptic bend discrete logarithm issue, one can accomplish the same cryptographic quality as calculations in view of the prime factorization issue, for example, RSA, utilizing shorter key lengths. Distinctive properties, for example, imperviousness to side channel assaults will vary between the bends utilized. A standout amongst the most widely recognized is Weierstrass, while different ones for example, Jacobian bends and Edwards bends will enhance distinctive properties of ECC. When utilizing equipment based ECC one is generally confined to the National Organization of Standards and Technology (NIST) - suggested bends, which has seen some discussion in late years [39]. There is a progressing banter about the responsibility for patent rights to ECC which may have hindered the appropriation of ECC somewhat [39]. While ECC has numerous potential utilize cases, it has seen the widest reception inside Public Key Cryptography (PKC).

Blowfish

It is a variable-length key block cipher. It doesn't meet every one of the prerequisites for another cryptographic standard talked about above: It is as it was reasonable for applications where the key does not change regularly, similar to an interchanges connect or, then again a programmed record encryptor. It is essentially quicker than DES when executed in 32-bit microchips with expansive information reserves, for example, the Pentium and the Power PC. This algorithm has two parts, a key-extension and date-encryption part. Key extension changes the key in sub-key clusters. Information encryption happens by means of a 16-round Feistel arrange. Each round comprises of a key dependent change, and a key-and information subordinate substitution. All operations are XORs and increases on 32-bit words. The main extra operations are four recorded exhibit information queries per round.

RC Cipher

RC remains for Ron's Code or Rivest Cipher. These figures were outlined by Ron Rivest for the RSA Data Security. Diverse RC Ciphers depicted quickly underneath.

RC2:

It was outlined as a brisk settle swap for DES that is more secure. It is a block cipher and also has variable key size that has appropriateness algorithm RC2 is a variable-key length cipher. Be that as it may, when utilizing the Microsoft base cryptographic supplier, the key-length is hard –coded to 40 bits. When utilizing the Microsoft upgraded cryptographic supplier, the key length is 128 bits naturally and can be in the range of 40 to 128 pieces in 8-bit increases.

RC5

RC5 is a block intended for speed. It permits a client characterized key length, information block size, and number of encryption rounds. In especially the key size can be as huge as 2,048 bits. RSA Data security is attempting to have RC5 incorporated into various web norms including 1Psec.

3.9 Comparison Different Classical Encryption Technique

Algorithm	**Type**	**Key/Hash in bits**	**Block in bits**	**Rounds**
RC4	Stream	128	8	128
IDEA	Block	128	64	8.5
RC5	Block	64	64	1-255
MD5	1-way hash	128	512	4

SHA1	1-way hash	128	512	80
AES	Block	128,192,256	128	10,12,14
DES	Block	56	64	16
Triple DES	Block	112,168	64	48
RC2	Block	40 to 1024	64	18
Blow Fish	Block	32 to 448	64	16
Skipjack	Block	80	64	32
ECC	-	160 to 512	-	-

Table 3.6-Comparison Different Classical Encryption Technique

CHAPTER 4

PRIVACY

Privacy is an umbrella term, alluding to a wide and unique gathering of related things [40]. Privacy, as indicated by Privacy International, is a multidimensional idea, which is identified with four segments they are body, communications, territory, and data. Real Privacy concentrates on the general population's physical assurance against any outer damage. Privacy of correspondences concentrates on the assurance of the data that is brought through any medium between two gatherings. This incorporates email, mail and phone. Regional Privacy is about building up limits or points of confinement on physical space or property, for example, the home, working environment, and open spots. Data security alludes to individual information that is gathered and prepared by an association, for example, medicinal records and Master-card data [41]. Privacy is that of somebody having the privilege to control what individual data gathered about them or, on the other hand known to others [42]. As innovation makes it trifling for associations to keep up extensive computerized records about each individual, Privacy concerns have risen. Individuals are worried about what information is gathered, who has admittance to it, which controls it, and what it is utilized for [43].

4.1 Privacy Threats

These days, it is considerably harder for us to hold our protection, as the Internet of Things innovations assume control over our everyday lives. Clashes over how associations can get to individual information are unavoidable, and IoT will add to this. Ziegeldorf's writing audit [44] lists the most well-known protection dangers in the Internet of Things:

1. **Identification** is the most overwhelming threat that interfaces an identifier, e.g. a name and address, with a person entity.

2. **Localization and tracking** are the threat of finding an individual's area through various means, e.g. GPS, web activity, or cell phone area.
3. **Profiling** is for the most part utilized for personalization in online business (e.g. in pamphlets and ads). Associations gather data about people to derive interests by relationship with different profiles and information sources.
4. **Interaction and presentation** alludes to the quantity of savvy things and better approaches for associating with frameworks what's more, showing criticism to clients. This turns into a threat to security when private information is traded between the framework and the clients.
5. **Lifecycle transitions** happen when an IoT things is sold, utilized by its proprietor lastly discarded. There could be a presumption that all data is erased by the protest, be that as it may, smart devices regularly store tremendous measures of information about their own particular history all through their whole lifecycle. This could incorporate individual photographs and recordings and are at times not endless supply of possession.
6. **Inventory attacks** apply to the unauthorized access to and gathering of information about the nearness and attributes of individual things. Robbers can utilize stock information to case the property to locate a protected time to soften up.
7. **Linkage** comprises in connecting diverse frameworks, the possibility of unapproved get to and breaks of private information develop when systems are connecting to join isolate information sources.

4.2 Privacy Preserving Solutions

Keeping in mind the end goal to address the privacy concerns of end-clients and privacy contemplations of specialist organizations, a few methodologies have been proposed by the examination group:

1. **Cryptographic techniques and information manipulation**: Despite the fact that analysts have spent numerous years proposing novel privacy-preserving plans, cryptography is as yet the prevailing one in most current proposed arrangements, despite the fact that, for the majority of the deterrents they may confront, a large number of the sensors can't offer satisfactory security protocols because of the restricted measure of capacity furthermore, computation resources [45].
2. **Privacy awareness or context awareness**: Solutions for privacy mindfulness have been predominantly centered on applications that give essential privacy mindfulness to their clients that smart devices, for example, smart TVs, wearable gadgets, and wellbeing screen system collect personal individual information about them. For example, in late research, a structure called SeCoMan was proposed to go about as a put stock in outsider for the clients as applications won't not be sufficiently dependable with the area data that they oversee [46].
3. **Access control:** Access control is one of the feasible answers for be utilized as a part of expansion to encryption and privacy mindfulness. This gives clients the ability to deal with their own information. A case of this approach is CapBAC [59], proposed by Skarmeta, Hernandez, and Moreno. It is basically a disseminated approach in which keen things themselves can make fine-grained approval choices.
4. **Data minimization:** The guideline of "information minimization" implies that the IoT specialist co-ops ought to restrict the accumulation of individual data to what is specifically pertinent. They ought to likewise hold the information just for

as long as is important to satisfy the reason for the administrations given by the innovation. At the end of the day, they ought to gather just the individual information they truly require, and ought to keep it just for whatever length of time that they require it [47].

There are other proposed solutions that don't fall into these four classifications, for example hitchhiking. This is a new way to deal with guarantee the obscurity of clients who give their locations Hitchhiking applications handle areas as the element of intrigue. Since the information of who is at a specific location is superfluous, the loyalty tradeoff is expelled [48].

Another case is the introspection technique that proactively secures clients' close to home data by looking at the exercises of the VM. It accumulates and breaks down the CPU state of each VM, the memory content, document I/O action, organize data that is conveyed through hypervisor and distinguishes malevolent programming on the VM. Nonetheless, if IoT gadget loses uprightness because of any vindictive assault, it makes dangers to the clients' security [49].

CHAPTER 5

OUTLINE OF PROPOSED SOLUTION

With the proliferation of IoT devices, the integration of these devices into the standard Internet introduces several security and privacy challenges. As IoT devices are constrained devices, they have less resources like memory, processing and power as compare to the traditional deices. That's why universal solutions to security and privacy problems that were initially intended for the Internet will not function because these solutions require a huge quantity of resources and energy, which constrained devices most likely do not possess. So there is need to upgrade the implementations designs to cop up security and privacy challenges in the IoT.

The fields of networking, communications, computing, hardware and software have change the way of people, smart objects, systems interact and exchange information. The Internet of Things will fuel the achievement of this new interconnected world. These systems strongly depends on the security and privacy of Internet of Things, as well as the sensitive data winded [4]. Although these technologies also offer many capabilities like the growth of hardware and software complexity, as well as the existence of global access, increase the vulnerability to security attacks.

5.1 Proposed Model for IoT

Proposed model for IoT security and privacy model show in figure 2. This model consists of a gateway, and all the IoT devices are connected to the network through this gateway. Gateway has the capabilities to connect to the outer world. It perform the operations like, Data Aggregation and communication between IoT devices and End user End user directly communicates to the gateway and further communicates to the IoT devices if it is a authenticated use.

This model also consist a middleware for solving the privacy issue in IoT systems, middleware is play important role for providing security and privacy in IoT system using cryptography, authentication, authorization and availability using technique Digital Certificate and OTP. This solution used the resource of server side for computations. This solution is suitable if network is secure data Transmission. This is best solution for small scale applications in IoT. Middleware is software implementation solution for IoT systems. Several requirements are handled by this middleware for privacy as confidentially, integrity, availability, authentication, authorization, access control using Digital Certificate and OTP.

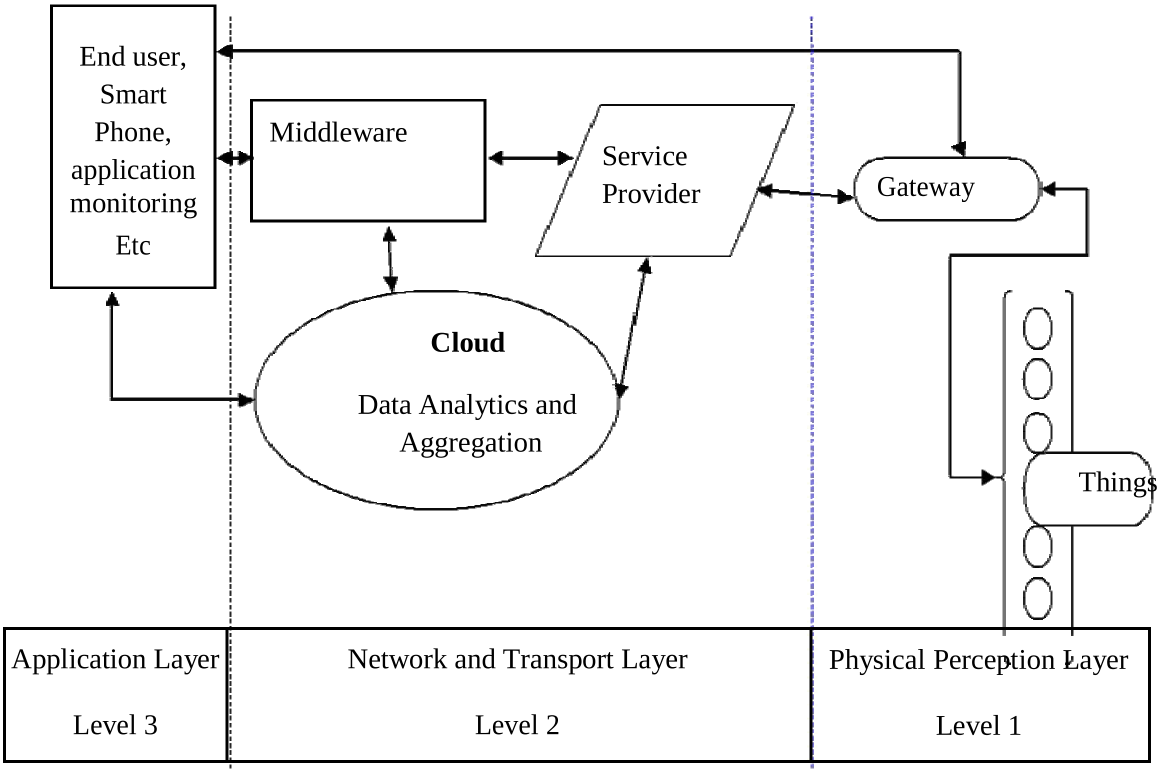

End user, Smart Phone, application monitoring Etc
Middleware
Service Provider
Gateway
Cloud
Data Analytics and Aggregation
Things
Application Layer
Level 3
Network and Transport Layer
Level 2
Physical Perception Layer
Level 1

Figure 5.1- Proposed Solution model for IoT

Here is a scenario of country security from terrorist, trying to enter in the country from borders. Here we need to increase the security by establishing the Long Range Body Heat Detector with IoT devices. These sensors detect the human Body heat and pass the information to the IoT device which is connected with the sensor. So in this case it is necessary to provide high level security to the IoT device.

5.2 Proposed Approach

Proposed solution for IoT shown in figure 2. This model consist constraint IoT devices and assuming they have limited recourses. In this solution Long Rang body heat detector is used, these sensors detect the human and pass the information to interconnected IoT devices. These devices have capability to encrypt the data by using Elliptic Curve Cryptography (ECC) and also apply CRC on the encrypted data to maintain the integrity of the data.

IoT device first Request (REQ) the Height Constraint Node (HCN) along with its RFID, for establishing the connection between them. HCN send its ID to IoT device to authenticate itself in the network. This node also send public key to IoT device by using Diffie Hellman key Exchange.

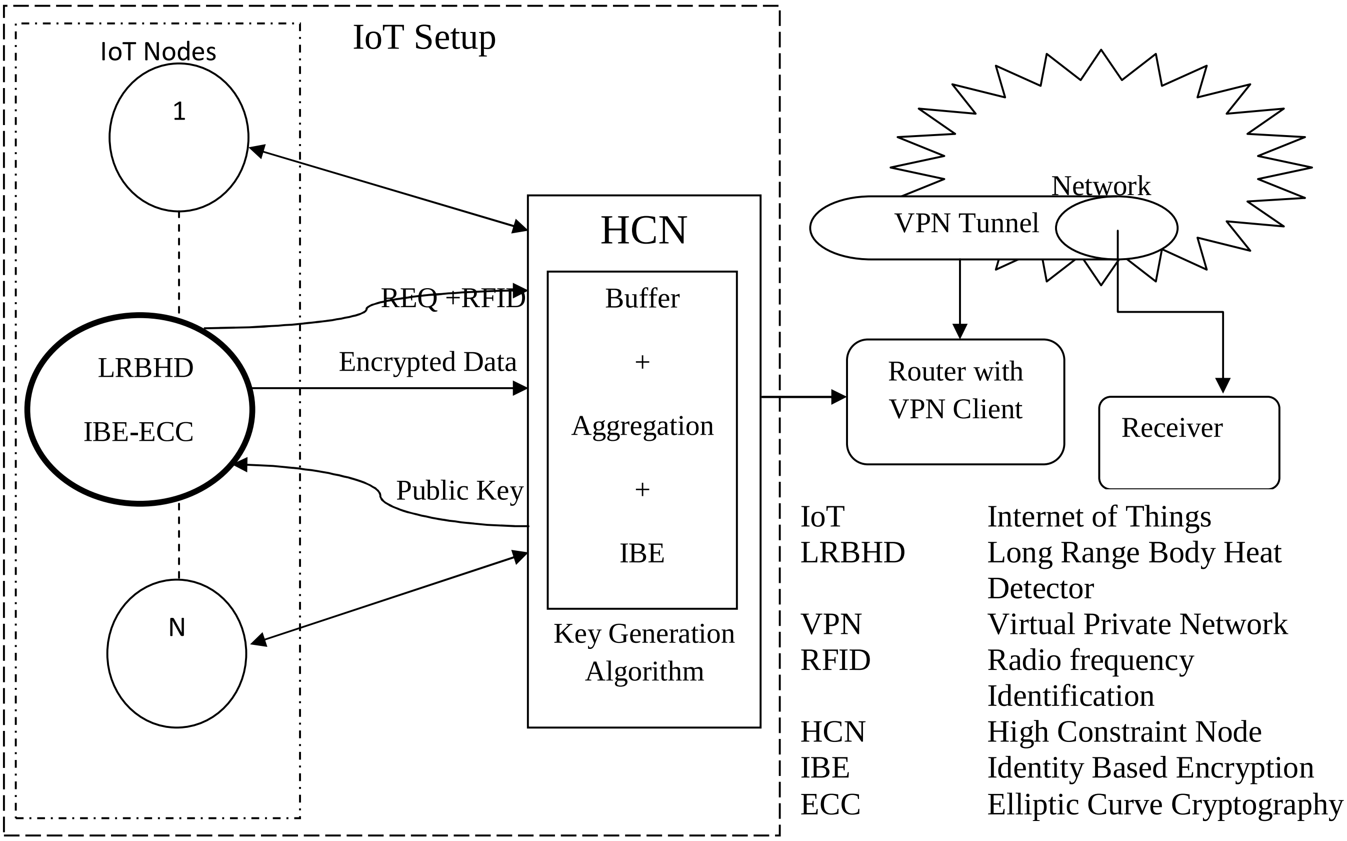


Figure 5.2- Proposed Approach for the scenario

IoT device encrypt the data by using public key for providing confidentially. After that IoT device also apply CRC technique on the data and attach checksum word along the data for maintain integrity and transmit it to the high constraint node.

Now, HCN collect the encrypted data from different interconnected nodes. This node maintain log file which conation the information of public and private key assigned to the different IoT devices, from this log file it decrypt the data of different Nodes and perform aggregation on the data. This HCN is further connected with the router with VPN client. This client has the capability to connect with the VPN tunnel and perform a secure and private communication between client server and receiver.

Through this approach security and privacy is provided to the IoT devices. Because all the communication is done between the IoT devices and HCN is encrypted. In this model I am using Identity Based Encryption with Elliptic curve cryptography (IBE-ECC). Identity Based Encryption is a vital primitive of ID-based cryptography. In that capacity it is a kind of public key encryption in which public key of a client is some one of a kind data about the character of the client (e.g. a client's email address). This implies a sender who has admittance to general society parameters of the framework can encode a message utilizing e.g. the content estimation of the recipient's name or email address as a key. The receiver acquires its decoding key from a central authority, which should be trusted as it produces secret keys for each client.

CHAPTER 6

RESULT ANALYSIS

In our technique we are using IBE with lightweight ECC for providing Security and privacy in single step for Internet of things for exchanging information between things and receiver. In our analysis we are comparing our technique with standard Encryption algorithms like AES, RSA and ECC. These results are analysis in between two IoT things and one high constraint node implemented in Virtual Machine, and Java Micro Edition installed in the machine. IoT`s generate fifty bytes of data and encrypt it. High constraint node collects the data and aggregates the data. From these results we analysis the time taken by the IoT devices to encrypt the data and time taken by the High constraint node to decrypt the data fifty byte.

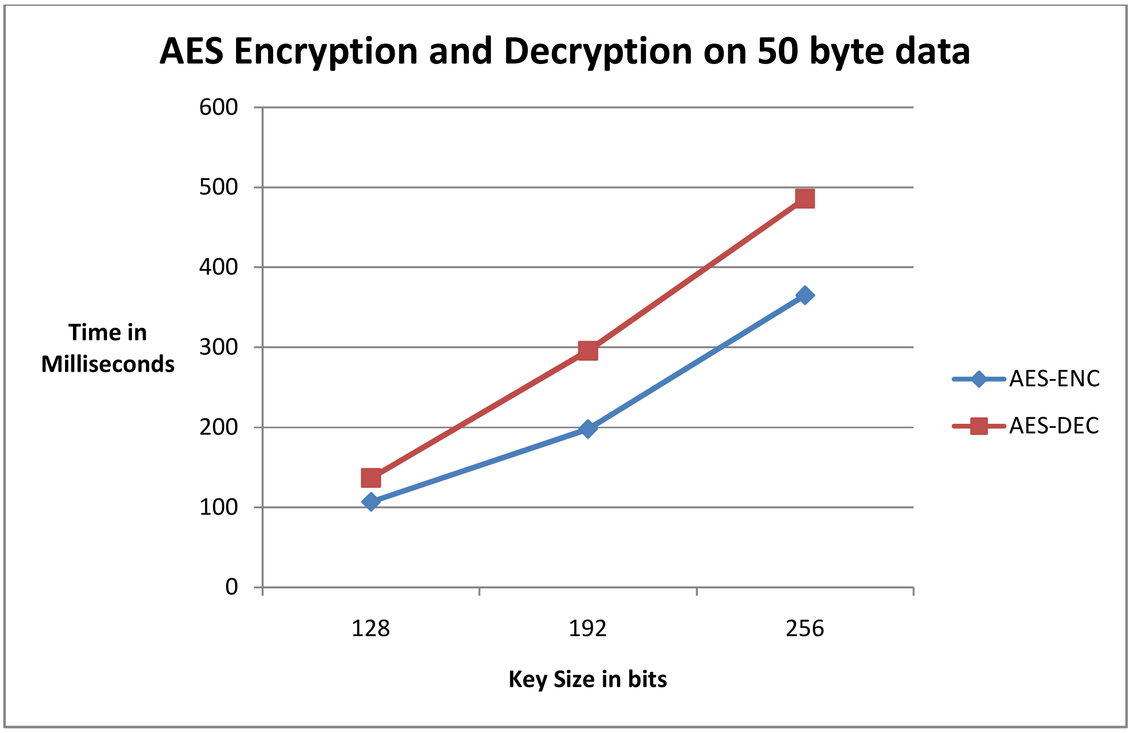


Figure 6.1 Time taken by AES in IoT

AES cryptography technique is suitable for IoT. But as the key size increases the number of rounds also increases and leads to increase the complexity of the system. So AES with 256 key size, may work in IoT but leads to high complexity

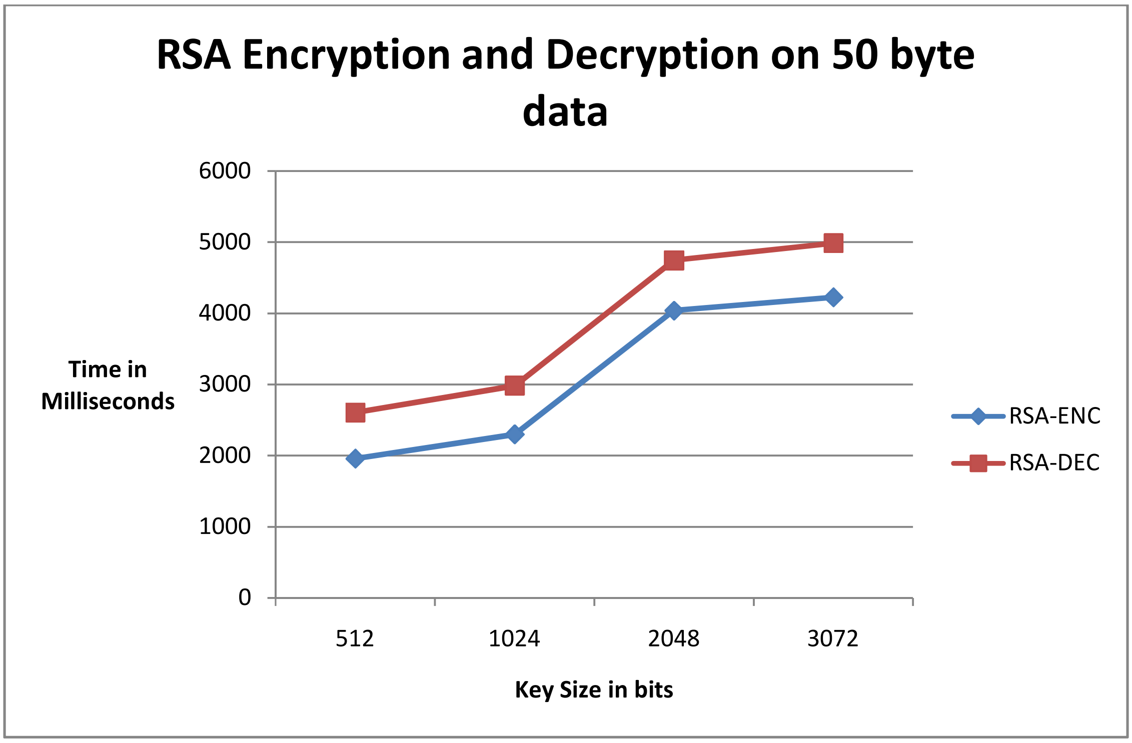


Figure 6.2 Time taken by RSA in IoT

RSA cryptography technique is not suitable for IoT due to large key size. In the case of IoT only RSA with 512 key size is suitable but it leads to increase the time complexity of the system.

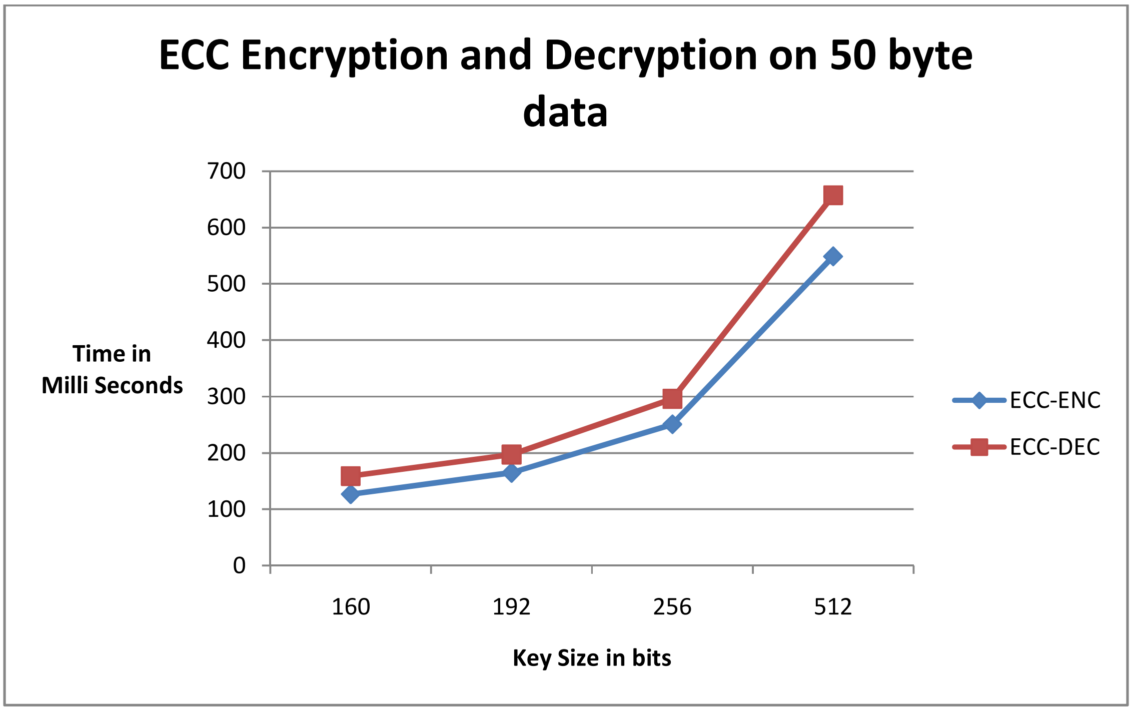


Figure 6.3 Time taken by ECC in IoT

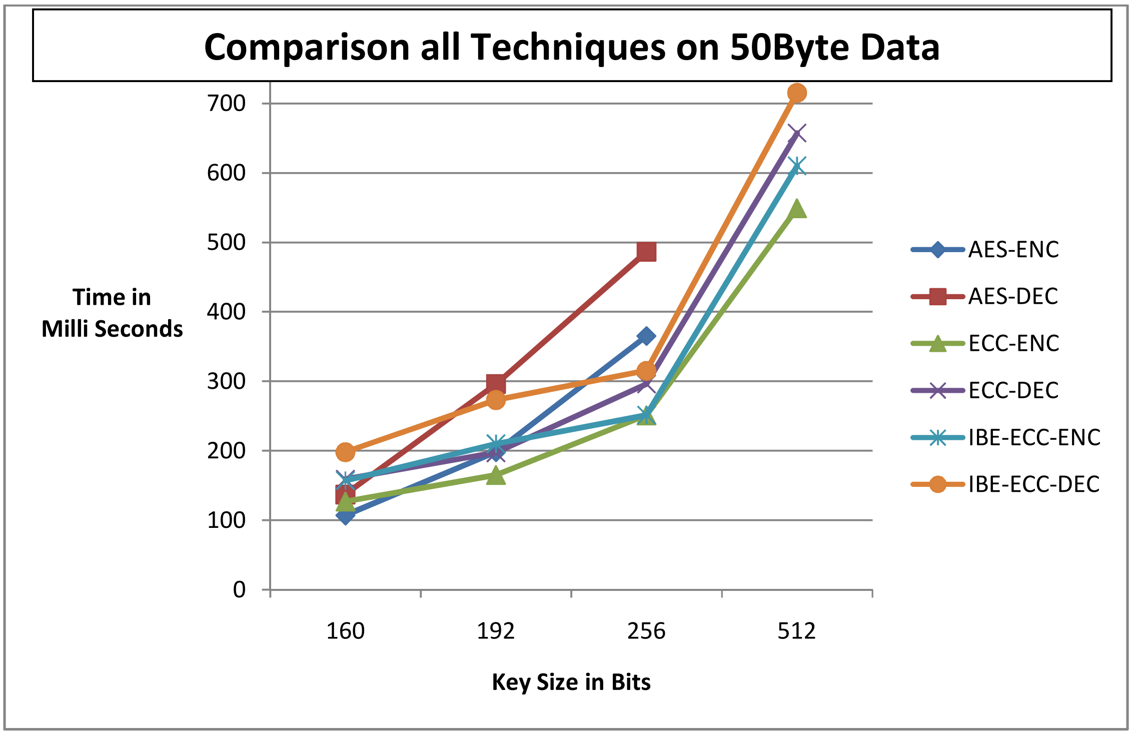


Figure 6.4 Comparison of Time taken different technique in IoT

This figure of compression show that AES 128 bit key size is suitable for IoT. But as the size of key is increased the number of round also increases which lead to make AES 256 bit unfit for the IoT. Our approach IBE-ECC 160 and 192 bit key is suitable for IoT as it take approximately equal time to ECC. But our technique provides security and privacy at same time because this approach use trusted third party called Private key Generator which generate private key and public key.

Table 5.1 shows comparisons between the different techniques and proposed approach based on different parameters.

Attributes	**Oualha [29]**	**Mao [30]**	**Lyes[17]**	**IBE-ECC**
Computation cost	Low	Low	high	High
Privacy	No	No	No	Yes
Trust	No	yes	No	Yes
Provide Storage space	No	Yes	Yes	No
Security	High	High	High	High
Technique	ECC	Fuzzy	ABE	IBE

Table 6.1 Comparison between different techniques

This table shows that IBE-ECC is better than other techniques in some parameters. Like this technique provide security, privacy and trust. But at the same time this technique requires high computational time and does not provide Storage space.

CHAPTER 7

CONCLUSION

7.1 Conclusion

As large devices are connecting day by day into a network, huge amount of data is also generated. So the success of IoT is strongly depends upon the security and privacy. In this thesis we have discuss about the IoT security, also discuss the Security architecture of IoT which further categorized in two types i.e. off -line architecture and On-line architecture and listed various attacks in IoT which distort the normal functioning of the IoT architectures. We have also listed some Lightweight cryptography techniques which overcome some of these attacks in the IoT. This thesis recognize the different lightweight encryption and unscrambling strategies and play out a tentatively investigation. In this postulation principally centered on the diverse lightweight encryption and unscrambling procedure utilized as a part of IoT for secure information transmission and improve the security of IoT. In this theory, clarified different security assault and significance of IoT in an everyday. Each system has a few focal points and weakness in IoT. Some strategy required more storage room yet less calculation the other way around. In this proposition analyze explore status of different lightweight encryption and unscrambling in IoT. Regular web is distinctive shape IoT; ordinary web is rich in its influence power, memory, stockpiling etc. where IoT is less influence, memory, and capacity. In postulation is attempted to locate the best lightweight encryption and unscrambling utilizing the authorization instrument. Our proposed model provides security and privacy to IoT devices by using PKG which distribute the key in the system. And we also compare our technique with other techniques which is suitable for IoT.

7.2 Future work

The Internet of Things is a generally new idea as far as upgraded conventions also, security, and consequently there is a great deal of work for what's to come. The most problem that is begging to be addressed is rearranging the utilization of security in IoT for engineers without exhaustive learning of IT security. Designing and implementing security in conventions that is basic for designers to utilize is an absolute necessity for the future of IoT. Speed and cryptographic quality is particularly essential in the Internet of Things. As gadgets in the Internet of Things are constrained devices, effective usage of cryptographic algorithms is particularly essential to keep the cryptographic quality at a satisfactory level. In this thesis we locate the best encryption and decryption technique that required minimum time for execution in IoT. In our proposed strategy required to enhance the encryption and decoding time that may functional appropriate for IoT. Form this analysis; this approach can be best suitable for the IoT environment.

CHAPTER 7

LIST OF REFERENCES

Journals

1. Ashton, K., 2009. That ‘internet of things’ thing. *RFiD Journal, 22*(7), pp.97-114.
2. Al Alkeem, E., Yeun, C. Y., & Zemerly, M. J. “Security and privacy framework for ubiquitous healthcare IoT devices”. *In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 70-75). IEEE. 2015, December.
3. Nia, A. M., & Jha, N. K. “A Comprehensive Study of Security of Internet-of-Things”. *IEEE Transactions on Emerging Topics in Computing*. (pp. 20-23). 2014 December

Conferences

4. Harris, Albert F., Hari Sundaram, and Robin Kravets. "Security and Privacy in Public IoT Spaces." In *Computer Communication and Networks (ICCCN), 2016 25th International Conference on*, pp. 1-8. IEEE, 2016.
5. SRI Consulting Business Intelligence/National Intelligence Council. Appendix F of Disruptive Technologies Global Trends 2025, 2008.
6. Nia, A. M., & Jha, N. K. “A Comprehensive Study of Security of Internet-of-Things”. *IEEE Transactions on Emerging Topics in Computing*. (pp. 20-23). 2014 December
7. Brachmann, Martina, Sye Loong Keoh, Oscar Garcia Morchon, and Sandeep S. Kumar. "End-to-end transport security in the IP-based internet of things." In*2012*

21st International Conference on Computer Communications and Networks (ICCCN), pp. 1-5. IEEE, 2012.

8. Bonetto, Riccardo, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples." In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, pp. 1-7. IEEE, 2012.
9. Al Alkeem, E., Yeun, C. Y., & Zemerly, M. J. "Security and privacy framework for ubiquitous healthcare IoT devices". *In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 70-75). IEEE. 2015, December.
10. Harris, Albert F., Hari Sundaram, and Robin Kravets. "Security and Privacy in Public IoT Spaces." In *Computer Communication and Networks (ICCCN), 2016 25th International Conference on*, pp. 1-8. IEEE, 2016.
11. Chen, Hsing-Chung, Ilsun You, Chien-Erh Weng, Chia-Hsin Cheng, and Yung-Fa Huang. "A security gateway application for End-to-End M2M communications." *Computer Standards & Interfaces* 44 (2016): 85-93
12. Arseni, Ştefan-Ciprian, Maria Miţoi, and Alexandru Vulpe. "Pass-IoT: A platform for studying security, privacy and trust in IoT." In *Communications (COMM), 2016 International Conference on*, pp. 261-266. IEEE, 2016.
13. Olivier, Flauzac, Gonzalez Carlos, and Nolot Florent. "New Security Architecture for IoT Network." *Procedia Computer Science* 52 (2015): 1028-1033.
14. Evans, David, and David M. Eyers. "Efficient data tagging for managing privacy in the internet of things." In *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on*, pp. 244-248. IEEE, 2012.
15. Wang, Xinlei, Jianqing Zhang, Eve M. Schooler, and Mihaela Ion. "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT." In *2014*

IEEE International Conference on Communications (ICC), pp. 725-730. IEEE, 2014.

16. Schurgot, Mary R., David A. Shinberg, and Lloyd G. Greenwald. "Experiments with security and privacy in IoT networks." In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*, pp. 1-6. IEEE, 2015.
17. 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.
18. 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.
19. Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 1996. *Handbook of applied cryptography*. CRC press.
20. 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.
21. 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.
22. 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.

23. 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.
24. 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.
25. 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.
26. 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.
27. Yalçin, T. "Compact ECDSA engine for IoT applications." *Electronics Letters*52, no. 15 (2016): 1310-1312.
28. Touati, Lyes, and Yacine Challal. "Collaborative KP-ABE for cloud-based internet of things applications." In *Communications (ICC), 2016 IEEE International Conference on*, pp. 1-7. IEEE, 2016.
29. 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.

30. Mao, Yijun, Jin Li, Min-Rong Chen, Jianan Liu, Congge Xie, and Yiju Zhan. "Fully secure fuzzy identity-based encryption for secure IoT communications." *Computer Standards & Interfaces* 44 (2016): 117-121.

31. Li, Fagen, Zhaohui Zheng, and Chunhua Jin. "Secure and efficient data transmission in the Internet of Things." *Telecommunication Systems* 62, no. 1 (2016): 111-122.

32. Tsai, Kun-Lin, Yi-Li Huang, Fang-Yie Leu, and Ilsun You. "TTP Based High-Efficient Multi-Key Exchange Protocol." *IEEE Access* 4 (2016): 6261-6271.

33. Adnan, Syed Farid Syed, Mohd Anuar Mat Isa, and Habibah Hashim. "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, 2016.

34. 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.

35. Yang, Ming, Nikolaos Bourbakis, and Shujun Li. "Data-image-video encryption." *IEEE potentials* 23, no. 3 (2004): 28-34.

36. Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." *Sony Corporation* (2008): 7-10.

37. Miller, Frederic P., Agnes F. Vandome, and John McBrewster. "Advanced Encryption Standard." (2009).

38. Somani, Uma, Kanika Lakhani, and Manish Mundra. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing." In *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on*, pp. 211-216. IEEE, 2010.

39. Bernstein, Daniel J., and Tanja Lange. "Security dangers of the NIST curves." In *Invited talk, International State of the Art Cryptography Workshop, Athens, Greece*. 2013.

40. Solove, Daniel J. "A taxonomy of privacy." *University of Pennsylvania law review* (2006): 477-564.

41. Stefanick, Lorna. *Controlling knowledge: Freedom of information and privacy protection in a networked world*. Athabasca University Press, 2011.

42. Westin, Alan F. "Privacy and freedom." *Washington and Lee Law Review* 25, no. 1 (1968): 166.

43. M. Langheinrich. Ubicomp 2001: *Ubiquitous Computing: International Conference Atlanta Georgia, USA,* September 30–October 2, 2001 Proceedings, chapter Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems, pages 273–291. *Springer Berlin Heidelberg, Berlin, Heidelberg,* 2001.

44. Ziegeldorf, Jan Henrik, Oscar García Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges." *Security and Communication Networks* 7, no. 12 (2014): 2728-2742.

45. Feng, Hailong, and Wenxiu Fu. "Study of recent development about privacy and security of the internet of things." In *Web Information Systems and Mining (WISM), 2010 International Conference on*, vol. 2, pp. 91-95. IEEE, 2010.

46. Lai, Chengzhe, Hui Li, Xiaohui Liang, Rongxing Lu, Kuan Zhang, and Xuemin Shen. "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service." *IEEE Internet of Things Journal* 1, no. 1 (2014): 46-57.

47. E. D. P. Supervisor. Data protection directive 95/46/ec.

48. Tang, Karen P., Pedram Keyani, James Fogarty, and Jason I. Hong. "Putting people in their place: an anonymous and privacy-sensitive approach to collecting

sensed data in location-based applications." In *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 93-102. ACM, 2006.

49. Kang, Chulhyun, Fizza Abbas, and Heekuck Oh. "Protection scheme for IoT devices using introspection." In *Network of the Future (NOF), 2015 6th International Conference on the,* pp. 1-5. IEEE, 2015.
50. Andress, Jason. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.
51. Bates, Regis J., and Donald W. Gregory. *Voice & data communications handbook*. McGraw-Hill, Inc., 2006.

Books

52. William Stallings , "*Cryptography And Network Security*" fifth edition Pearson publication (PP-35).