SECURITY ARCHITECTURE OF INTERCONNECTED SMART DEVICES,

AN ANALYSIS OF SECURITY ISSUES WITH SOLUTIONS

by

Bilal Javed

A thesis submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Computer Sciences

Dec 2016

SUPERVISOR'S CERTIFICATE

It is certified that the final copy of thesis has been evaluated by me, found as per specified format and error free.

Dated: _____ 2016

_____
(**Col Imran Rashid, PhD**)

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

_____

(Bilal Javed)

ABSTRACT

Internet is a global network of computing systems and smart devices which utilizes standardized protocols to create services for end users. It shapes “network of networks” which comprises of public and private network connected by employing variety of wireless, wired and optical communication technologies. Internet of Things (IoT) is the evolution of Internet and is considered as future of Internet. IoT is characterized by its heterogenous nature where billions of smart devices, sensors, embedded computers, actuators and people are interconnected to interact among themselves and with their environment. In IoT paradigm, when devices termed as “Things” are provided with Internet connectivity then it becomes IoT with the aim to converge physical and virtual world for prescribed services. Moreover, various standard bodies and consortium are contributing to standardized IoT protocols and communication technologies. Unlike traditional computing systems, IoT objects are designed to perform prescribed functionality by employing needed resources to keep procurement and implementation cost low.

The wide range of smart entities, diverse nature of IoT communication and existence of imbalance resources among IoT objects creates immense challenges and security issues for IoT ecosystem. Moreover, availability of various IoT standards and non-availability of unified agreed upon standard also poses challenges for IoT implementation. Compared to traditional computing systems, resources in terms of processing, memory, power and bandwidth capacity are limited in IoT environment therefore security mechanisms designed for regular computing system are impractical and not always applicable for implementation in IoT ecosystem. Hence, security is a prime concern which must be addressed for IoT success and to reap its potential benefits.

This thesis examines the building blocks needed for IoT architecture. Deployment strategies have been explained with a view to carry out their impact and security analysis. This research contributes in security analysis of IEEE 82.15.4, 6LoWPAN, RPL and CoAP so as to highlight areas for optimization and improvement of security aspect. In this study, IoT standardization has also been discussed from different angles in order to proffer recommendations for unified IoT standard. Different IoT gadget and products which are available in the market are examined from security perspective. This research also explains various security challenges and issues pertaining to IoT. Finally, solutions to security challenges and issue to IoT are proposed which includes design considerations, framework for key establishment schemes in constrained devices, a model for centralized IoT deployment and security guidelines for IoT environment.

ACKNOWLEDGMENT

Submission of this thesis brings and end to a wonderful phase of my life in Military College of Signals (NUST) where I remained a student of MSIS (Information security). Over the years, this incredible institution has imparted finest of training and quality education throughout my military carrier.

This research provides an opportunity for me to explore new avenues and facilitated to improve existing knowledge pertaining to Internet of Things (IoT). I extend my gratitude to all faculty members for their unflinching efforts and remarkable commitment to impart quality knowledge which has enabled me to accomplish this study.

My greatest of appreciation and gratitude to my thesis supervisor Colonel Imran Rashid, PhD for his support, trust and confidence for making this thesis possible. It was his encouragement and guidance which facilitated to formulate this research. At the same time, I am also grateful to Assistant Professor Mian Muhammad Waseem Iqbal and Lecturer Waleed Bin Shahid for their time, advice and guidance.

I am deeply grateful to all my family members for the encouragement, care and support. Especially, I will be forever thankful to my parents for their devotion and all the things they done for me.

Last but not the least, in my humble capacity I am very much grateful to Almighty Allah for all the blessing He bestowed upon me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

The goal of this chapter is to explain Internet of Things (IoT) and the role of smart interconnected devices in IOT paradigm. The potential of IOT is limitless and has application in different field of life which are enumerated in order to comprehend its potential impact. Wide application range and potential benefits has contributed towards its popularity therefore based on reports, future prospects have been discussed. Several challenges exist in IoT domain which has become motivational factor. Research objectives and its contribution towards research community is elucidated in this chapter. Finally, problem statement has been drawn and thesis outline is given to provide an overview of complete study.

1.1 Introduction

Internet is a global network of computer and smart devices which utilizes standardized protocols to create services for end users. It forms "network of networks" comprises of public and private networks connected by variety of wireless, wired and optical communication technologies. In present day world, connected devices are becoming essential part of human life due to which demand of internet in increasing with each passing day. Relatively a new concept of interconnected devices has emerged called as "**Internet of Things**" also considered as future of internet [1], [2].

Notion of Internet of Things (IoT) was initially proposed by Kevin Ashton in 1998 that allows people and smart devices to communicate anytime, anyplace, with anything and anyone by utilizing any network and any service [2]. IoT is the evolution of Internet which is seizing a gigantic leap to collect, analyze and distribute data which can then turn it into information, eventually into wisdom. IoT is one of the promising solutions to meet the requirement of autonomous device communication and collaboration. IoT creates an ecosystem which enables realization of human vision in terms of (i) Smart Building where windows, gates, locks, doors, lights and other things are controlled remotely and locally (ii) Smart Grid which improves efficiency of electricity distribution and production for

consumers (iii) Smart Cities, enabling efficient management of street lights, traffic flow, parking and other services within the city. So, major utility of IoT is to sense, data collection, data processing and responding in a beneficial manner for end users [2], [3].

1.2 Internet of Things (IoT)

IoT refers to a network of uniquely identifiable and interconnected smart devices which constantly gather data for prescribed operation and intended services. Concept of IoT is to meet human needs by utilizing sensors and devices into a network to automatically generate notification or to perform preset functionality. As per Wikipedia "The Internet of Things is the internetworking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators and network connectivity that enables these objects to collect and exchange data" [4]. IoT European Research Cluster (IERC) defines IoT as "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities, and use intelligent interfaces, and are seamlessly integrated into the information network" [5]. Likewise, IoT has been defined in Recommendation ITU-TY.2060(06/2012) as "A global infrastructure for the information society, enabling advanced services by interconnectivity (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [6].

It is the smart devices and their interconnectivity, which are the core components of IoT for intended services and functionality. As shown in figure 1.1, IoT network can be categorized as Personal Area Network (PAN), Local Area Network (LAN) and Wide Area Network (WAN) where different smart objects interact with each other for their intended operation. The concept of IoT is to meet human needs by customizing sensors or devices placed within a network, so that they can automatically send important notifications on occurrence and perform preset operation without human intervention. The potentials of IoT are limitless, the most fascinating phenomenon materializing within the cyber space. IoT has its application in all fields of life and has bright future prospects in term of adoption [7]. So, in coming years the internet will see a huge growth in interconnected devices but with this growth cyber-attack surface will also rise as compared to present day cyber world. This highly interconnected network of smart devices will bring along and create more security challenges for IoT devices and the networks in which they operate. An important aspect of IoT device is its constrained resources in terms of processing, power, memory and bandwidth capacity due to which traditional security solutions and

protocols which requires considerable resources therefore not always applicable in IoT constrained environment.

Figure – 1.1: Network Range of IoT

1.2.1 Applications of IoT

IoT is the future of Internet where business, government and consumer will not only interact with each other but with the physical world as well [7]. IoT will have huge impact on broad range of market sector as shown in figure 1.2, including but not limited to following: -

- **Military**: IoT technology can be employed in military to monitor troops activity, to manage resources and their allocation, administer IT infrastructure, supervise storage facilities etc.
- **Agriculture**: IoT can have enormous impact on agricultural sector in terms of soil analysis, management of crops etc.
- **Industry**: Industry can make use of IoT in the form of smart meters, sensing location, assessing equipment performance, controlling and monitoring operations, controlling and monitoring HVAC (heating, ventilation and air conditioning) etc.
- **Retail Services**: IoT technology can be used for tracking of assets, maintaining inventory, marketing and to manage supply chain.

- **Environmental**: IoT can be utilized for tracking the endangered species, predicting the weather and resource management.
- **Automotive**: IoT has its potential in automotive field in terms of city traffic flow, management of parking, smart key entry, vehicle location, monitoring vehicle health and anti-theft etc.
- **Smart Homes**: IoT can be utilized in making of smart home to control lightning, security gadgets, heating, air conditioning etc.
- **Healthcare**: IoT can be employed for telehealth, implanted and wearable devices etc. Devices like Fitbit and Jawbone are available in the market, helping people to manage their fitness by providing data pertaining to their workout.

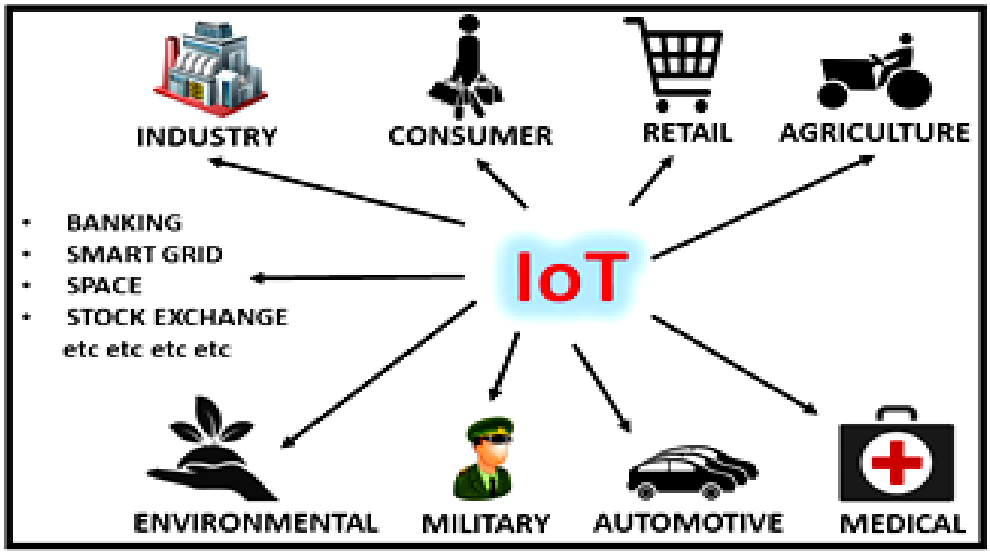

Figure – 1.2: IoT Applications

1.2.2 Future Prospects of IoT

As per Business Insider tech report published in August 2016, it is projected that by 2020, at around 34 billion devices will be connected to the internet. Moreover, it is estimated that in the next five years nearly $6 trillion will be invested in IoT sector [8]. Various businesses around the world will prefer to embrace IoT due to low operational cost and increased productivity. Likewise, governments will also adopt IoT in order to improve quality of life for their citizens. As far as end users are concerned, they will spend healthy amount in purchasing IoT devices and for their associated services.

Similarly, according to Verizon report “State of the Market: Internet of Things 2016” published in April 2016 states that IoT market spending will grow from $591.7

billion which was in 2014 to an estimated $1.3 trillion by 2019. This shows a composite growth of 17 % annually in IoT technology. As far as installation of devices are concerned, the state was 9.7 billion in 2014 which is likely to increase more than 25.6 billion by 2019, reaching more than 30 billion devices in 2020 all around the world [9].

Keeping in view the application of IoT in the market, device production, investment in technology, academia contribution and potential return on investment; the prospect of this technology are very bright and high. Approximate projection of IoT in coming years is as shown in figure 1.3. The graphical representation shows exponential growth of IoT device where by year 2020 the number of devices will cross 30 billion devices all around the world. With this exponential growth, attack surface and attack vectors will also increase as compared to present day internet. Practical manifestation of which the world has recently seen in term of DDoS attack on cyber security blog called as "Krebs on Security" in September 2016 where 650 Gbps of traffic was directed against the site. Similarly, on 21 October 2016 DDoS attack was materialized against "Dyn", a Domain Name Server for Twitter, GitHub, PayPal, Amazon, Reddit, Netflix, and Spotify where approximately 100,000 devices used also including IoT Botnet.

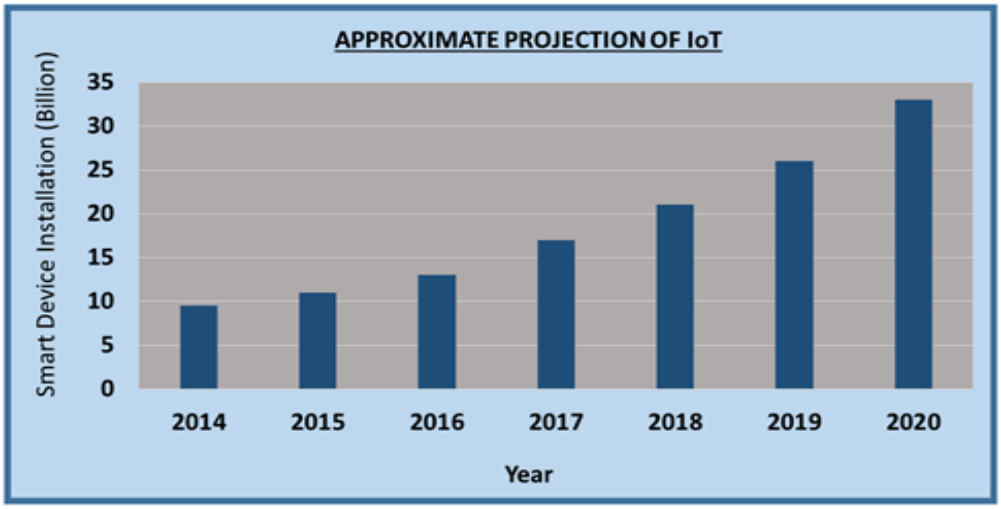

Figure – 1.3: Estimated Growth of IoT

1.3 Motivation

Internet of Things (IoT) consist of billions of people, smart devices and services which have the potential to interact among themselves and with their environment. It is expected that IoT markets will surge in coming years bringing millions of new IoT devices online and will create network of networks. This highly interconnected global network structure raises new types of challenges from a security, trust and privacy perspective.

Similarly, huge scale interconnectivity will also increase attack vectors and attack surface for the adversaries to exploit IoT devices along with the network in which these devices installed. Moreover, traditional security mechanisms are difficult to implement for security of IoT environment due to constrained resources such as computational power, energy, memory and bandwidth. In this context, this study is motivated by the need to create security by design and achieve efficient and cost effective security mechanisms pertaining to IoT architecture. This research concentrates on achieving embedded security, smart device security and security of IoT network keeping in view confidentiality, integrity and availability requirement.

1.4 Thesis Objectives

Research methodology employed in this thesis is based on analytical research to evaluate and to carry out security analysis of different concepts, technologies and services pertaining to IoT, followed by solution to security challenges. The objectives of this thesis are: -

- To describe building block which form the basis of IoT.
- Deployment strategies of IoT devices in a network, their impact and security analysis.
- Analyze existing protocols of IoT with regards to security.
- Analyze IoT standards and problem in their acceptance.
- Security analysis of current IoT products and services in the market.
- To identify, study and analyze security issues and challenges to IoT.
- Solutions to security challenges and issue to IoT.

1.5 Thesis Contributions

This study involves security analysis of different aspect of IoT with the purpose to offer solutions to security challenges and issues pertaining to IoT. The main contributions of this thesis are: -

- Security analysis of IoT deployment approaches.
- Security analysis of major IoT protocols.
- IoT standardization and problem in acceptance for vendors and manufacturers.
- Identification of security challenges and issues pertaining to IoT.
- Solution to security challenges and issues in IoT, which includes: -
  - Design considerations for developers / manufacturers to achieve embedded security.

- Central Management Unit in IoT network to achieves security and to address challenges in network.
- Two frameworks for lightweight Key Establishment schemes involving Out of Band (OOB) challenge and Trusted Third Party.
- Security guidelines and best practices for IoT security.

1.6 Problem Statement

Internet of Things (IoT) is a collection of large numbers of smart devices and services having potential to interact among themselves and with their environment. IoT ecosystem is characterized by resource constrained nature where devices are constrained in terms of computation capability, power, memory and bandwidth capacity. Hence, IoT devices do not support traditional security mechanisms which require considerable resources. So, challenges to resource constrained devices appears in the form of: -

- Embedded security.
- Interoperability of devices in IoT network.
- Identity management of devices.
- Secure pairing, authentication and authorization.
- Protection against internet borne attack.
- Protection of devices with IoT network.
- Challenges to layered security.
- Key establishment in IoT constrained environment.

1.7 Thesis Outline

This thesis "**Security Architecture of Interconnected Smart Devices – An Analysis of Security Issues with Solutions**" is organized in ten chapters.

Chapter 2 includes literature review and background information pertaining to IoT, Wireless Sensors Network (WSN), Machine to Machine (M2M) and other protocols. In **chapter 3**, building blocks which forms the basis of IoT are examined and explained. **Chapter 4** describes deployment strategies (Central and Distributed) of IoT devices in a network. Impact and security analysis of both the approaches are proffered. **Chapter 5** deals with security analysis of major IoT protocols. **Chapter 6** deals with IoT standardization and their impact analysis. **Chapter 7** carries out analysis of IoT products and services available in the market with regards to security concerns for consumer. In **chapter 8**, various security challenges and issues pertaining to IoT are discussed. Finally, **chapter 9** proposes solutions to security challenges and issues relating to IoT.

CHAPTER 2
BACKGROUND

In this chapter, required technical aspect have been explained in order to understand technical side of IoT. Topics which have been covered are pertaining to different concepts, protocols and communication technologies of IoT.

2.1 Wireless Sensor Network (WSN)

Wireless Sensor Network (WSN) is a collection of smart devices in a network communicating among themselves using wired or wireless medium. Individual sensor called as "node" may have the ability to sense, communicate, connect and process sensed data whether locally or remotely. WSN creates wireless infrastructure with the objective to detect event or sense the environment which occurs in monitored zone and delivers the sensed data to dedicated gateways called "sink" which eventually transfer the collected data to cloud or management units. WSN architecture can be deployed using centralized and distributed approach in IoT perspective. In centralized approach, a central entity (server or cloud service) receives acquired data from sensors, process it and transform the data in appropriate format. In centralized deployment, there is little or no support of directly accessing the device or data from it. On the other hand, in distributed WSN approach the raw data is directly accessible from sensors due to sufficient processing power and communication mechanisms. WSN has wide application range such as military, industry, health, home and others. Normally nodes are small and cost effective, so their processing ability, power and memory are constrained. It is because of constrained nature; traditional security mechanisms and solutions are difficult to implement in WSN environment [10].

2.2 Machine to Machine (M2M)

Machine to machine (M2M) connectivity involves technology and mechanism which allows network devices to exchange data and perform prescribed functionality with minimal human intervention. M2M extends sensor networking model which represent advanced network for data exchange among physical devices without human involvement. M2M can be characterized by three features i.e. smart devices, automated operation and distributed communication. First, M2M involves variety of smart objects

ranging from constrained devices to resourceful servers. Second, autonomous operation of devices without human intervention. Third, M2M uses distributed communication methodology where two nodes create connectivity among themselves offering service or resources at the other end [11].

Compared to WSN, communication does not follow hierarchical path (WSN: sensor to sink, sink to gateway) in M2M but directly communicates with other nodes irrespective of distance, role and capabilities. The scope of M2M application includes smart grid, e-health and so on therefore usually considered as subset of IoT.

2.3 Internet of Things (IoT)

IoT is an innovative model which enables huge number of smart devices to be connected to Internet. These devices can be sensors / actuators with the ability to operate and exchange data with or without human intervention. Notion of IoT initiates vision of "future Internet" where end users and smart devices maintaining sensing and actuating abilities interact and collaborate with exceptional convenience and in economical manner. IoT has many applications in every sector of life such as medical, banking, transportation, smart homes, smart cities and so on. With the passage of time it is expected that IoT will have substantial impact on home, cities, industry, business and other sectors while contributing towards improved quality of life and to expand global economy. In order to achieve this potential development, promising technologies and innovations along with service applications needs to grow proportionally to meet market demand and consumer requirements. As IoT devices are connected to Internet therefore extend services and information to anyone, at anytime and anywhere [2].

Standardization of IoT architecture is a backbone to establish environment for vendors and manufacturers to offer state of the art and cost effective IoT products [12]. In addition, security is another important factor for the success of IoT which is challenging to achieve due to integral heterogeneity of connected smart devices with the ability to perform prescribed functionality. As IoT devices have limited resources in terms of processing, power, memory and bandwidth therefore implementation of security mechanisms is challenging. Furthermore, management and supervision is yet another prime factor to deliver quality services to end user at manageable cost.

2.4 Home Automation

We live in our homes and enjoy the comfort of life offered by technologies such as lights, air conditioning, microwave ovens, refrigerator and others. There can be several advantages if these gadgets are made autonomous and to respond to human behavior.

This automation is termed as “Smart Home” or “Intelligent Home Automation System” which utilizes WSN, M2M and IoT technologies. Generally, smart home is a collection of sensors which collect data or sense the event and then based on collected data prescribed functionality is carried out as per the needs of inhabitants [13].

2.5 IEEE 802.15.4

This protocol was designed to specify Medium Access Control (MAC) and Physical Layer (PHY) communication for low rate wireless personal area network (LR-WPAN). As IEEE 82.15.4 creates specification for low data rate, low cost, low power consumption and high through put therefore used by WSN, M2M and IoT. IEEE 802.15.4 specifies three frequency channels by utilizing Direct Sequence Spread Spectrum (DSSS) technique. Physical layer transmits and receive on three data rates i.e. 250 kbps at 2.4 GHz, 40 kbps at 915 MHz and 20 kbps at 868 MHz. In order to avoid collisions, MAC layer uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. This standard supports two types of smart devices i.e Full Functional Device (FFD) and Reduced Functional Device (RFD). The FFD can act as coordinator or just node where it can store routing table and implement MAC. On the other hand, RFD are resource constrained devices and can only communicates with coordinator or controller [14], [15].

2.6 IPv6 Low Power Wireless Personal Area Network (6LoWPAN)

IoT connects smart devices to Internet for which IP is the backbone for global connectivity. As constrained networks are getting IP enabled therefore shifting from isolated WSN and stepping towards global connectivity. For IP packets to be routed in constrained environment such as IEEE 802.15.4 based network, IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) has been specified [16]. As IEEE 802.15.4 mandates Maximum Transmission Unit (MTU) size of 128 bytes and spare 120 bytes for data transmission at higher layers therefore cannot be supported by IPv6 protocol which mandates MTU of 1280 bytes. To handle this, 6LoWPAN offers methodology of mapping between traditional IP networks and IEEE 802.15.4 based network by means of: -

- Header compression, which specifies the mechanism to compress IP and UDP header to reduced payload.
- Fragmentation, which defines the fragmentation and assembling of IP packets larger than IEEE 802.15.4 MTU size.

2.7 Routing Over Low Power and Lossy Network (RPL)

Internet Engineering Task Force (IETF) routing over low power and loss link working group defined a standard for routing of packets in resource constrained ecosystem called RPL. Routing of fragmented packets over 6LoWPAN protocol is managed by this protocol. RPL is specified to support routing needs for simple and complex traffic models like multipoint to point, point to point and point to multipoint. In this regard, Destination Oriented Directed Acyclic Graph (DODAG) is the core element of RPL where each node in DODAG is aware of its own position and location of other nodes involved in routing of packets. Four type of control messages are used in RPL to maintain routing topology and to keep routing information updated. First, DODDAG Information Object (DIO) is used to maintain information pertaining current level of node, determine the distance of each node to route and selection of preferred path. Second message is Destination Advertisement Object (DAO) for upward and downward traffic by giving its destination information. Third, DODAG Information Solicitation (DIS) which is used by the device to get DIO message. Fourth message is DAO Acknowledgement (DAO-ACK) which is transmitted in response to DAO message.

DODAG starts when the root node sends its position utilizing DIO message to all low power lossy network (LLN) levels. At every level, receiving routers notes parent path and participation path for all the nodes. Similarly, they send their own DIO message and consequently DODAG is constructed for entire network [17].

2.8 User Datagram Protocol (UDP)

Networks and applications based on Internet connectivity employs TCP protocol at transport layer in OSI model. TCP has the advantage that it guarantees delivery of packets to its destination but at the same time has large overhead on communication and processing resources. So, TCP is not suitable for resource constrained environment. To address, User Datagram Protocol (UDP) is preferred protocol for IoT in transport layer as it is connectionless protocol and do not puts constraint on limited resources [18].

2.9 Datagram Transport Layer Security (DTLS)

HTTP is a widely utilized web protocol which operates over connection oriented TCP. For end to end security, TLS is employed that prevents threats like eavesdropping, tampering or message forgery. On the other hand, UDP is used for IP based resource constrained networks due to low overhead on communication and processing requirements. For security required at transport layer for constrained network, Datagram

Transport Layer Security (DTLS) has been specified by Internet Engineering Task Force (IETF).

DTLS is based on TLS which provides equivalent security measures like confidentiality, authentication and integrity. TLS utilizes TCP thus does not confront packet loss and packet reordering. However, in DTLS packet loss is handled by retransmission timer whereas packet reordering issue is resolved by assigning a sequence number to each handshake message. DTLS mechanism consist of initial authentication of devices, key agreement and finally protection of data through secure channel. It is highlighted that initial DTLS handshake is expensive on resource constrained devices [18]. DTLS handshake is as under: -

1) Client initiate handshake using “ClientHello” message which contains security parameters and random value.
2) Server receives “ClientHello” message and generate cookie in the form of HMAC (Secret, Client-IP, Client Parameters) and send it to client in “ClentHelloVerify” message.
3) Client in return repeats the same “ClientHello” message with cookie included.
4) Server receives “ClientHello” with cookie, it then verifies the cookie sent by client. If cookie is valid then server generates random number and sent it to client in “ServerHello” message.
5) Server also send “ServerCertificate” message which includes certificate signed by certificate authority (CA) for authentication followed by “ServerKeyExchange” message.
6) Client after receiving the certificate, extract public key of server.
7) Server also send “CertificateRequest” followed by “ServerHelloDone” message.
8) Client send its certificate for authentication followed by “ClientKeyExchange” message containing parameters to generate pre-master secret.
9) Client send “CertificateVerify” message with a purpose that it has private key corresponding to public key.
10) Based on pre-master secret and other parameters exchanged earlier, Master key is derived at both ends.
11) The “ChangeCipherSpec” message from both client and server indicates that further communication will be encrypted with Master Key.
12) The “Finished” message from both the entities shows that they have agreed to communicate over this secure channel.

2.10 Constrained Application Layer Protocol (CoAP)

HTTP which is based on client / server model is commonly used protocol on application layer. This protocol is used over TCP and does not work with UDP. Furthermore, HTTP requires computational resources and not suitable for resource constrained environment. To address this challenge, IETF Constrained RESTful Environments (CoRE) has specified protocol called “CoAP” at application layer which can be employed over UDP [19]. CoAP is tailored to meet the requirements of resource constrained microcontrollers and in WSN, M2M and IoT environments. For security purposes, DTLS protocol is recommended to use for secure traffic.

CoAP utilizes set of techniques to compress application layer protocol metadata without conceding application interoperability by using representational state transfer (REST) architecture. The CoAP specifies request and response model among applications and allows the use of Universal Resource Indicator (URI) addresses for identification of resources available on constrained devices. CoAP supports communication at application layer between constrained devices and other entities on Internet using only CoAP or by translating HTTP to CoAP utilizing gateway. Messaging in CoAP is as under: -

- Confirmable message request is directed when client is expected to receive response or delivery confirmation. The response can be non-confirmable or acknowledgement message or both of these messages.
- A non-confirmable message request is send once client does not require a confirmation of request.
- Acknowledgement message is sent as a reply to verify that request was delivered.
- A reset message is sent as a reply to confirmable or non-confirmable device to inform that request was received but some data was lost.

2.11 IEEE 802.11i

WiFi is a technology which enables devices to connect to wireless LAN (WLAN), mainly employing 2.4 GHz and 5 GHz frequency [20]. WiFi Alliance describes it as any “wireless local area network (WLAN) product which is based on Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards”. Devices which implements WiFi technology include smart phones, computers, tablets, cameras, audio players and so on. WiFi enabled devices connect to Internet utilizing wireless access point (AP). WiFi uses security mechanisms in terms of Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) and WiFi Protected Access 2 (WPA2).

In WEP standard, security is implemented using RC4 stream cipher. But it has shown severe weakness as it uses short initial vector (IV) which makes security easy to break. Next security standard introduced is called WPA, which has adopted Temporal Key Integrity Protocol (TKIP) and per packet key. Hence, becomes more secure than WEP. WPA was introduced as an intermediary solution to WEP flaws. Finally, IEEE 802.11i standard was introduced also known as WPA2 which utilizes Advanced Encryption Standard (AES) giving more security compared to WEP and WPA. Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is used which provides both confidentiality and data integrity. WPA2 has two components i.e. encryption and authentication, encryption component mandates AES utilization whereas authentication component uses Personal and Enterprise mode.

WPA2 creates secure communication in four phases. First, AP and client agree on security policy. Second, applicable to Enterprise mode only where 802.1X authentication is started between client and AP, then generates master key. In third phase, temporal key is computed after successful authentication which is regularly updated. Fourth, all computed keys are used by CCMP for data confidentiality and data integrity.

2.12 Bluetooth Low Energy (BLE)

Bluetooth offers communication mechanism which is used to exchange data among devices over short distances using short wave length to minimize power consumption [21]. Bluetooth Low Energy (BLE) utilizes short range radio with minimum amount of power to function for longer duration compared to earlier versions [22]. Transmission power between 0.01 mW to 10mW can be used to operate BLE. In this context, BLE is efficient communication technology for resource constrained devices.

Physical Layer (PHY) stack in BLE is to transmit and receive bits. Above PHY stack, link layer operates which enables medium access, establish connection, allows error control and flow control. After this, Logical Link Control and Adaptation Protocol (LLCAP) enables multiplexing, fragmentation and reassembly of packets. Other upper layer includes Generic Attribute Protocol (GATT) offers collection of data and Generic Access Profile (GAP) which allows configuration and functioning in different modes.

In BLE network, devices operate as master and slave. The slave transmit advertisement for discovery which are scanned by master device. When two devices are connected, and communicating data then other devices remain in sleep mode to conserve power.

2.13 Z-Wave

It is a low power wireless communication technology designed to be used in home automation and small size commercial units. Coverage range of Z-wave is about 30 meters and is designed for devices to transmit less data such as fire detectors, ambient control devices, HVAC systems, access control devices and others. Data rate is 40 kbps in Z-wave which functions in ISM band using 900 MHz frequency. The MAC layer of Z-wave has collision avoidance mechanism and reliability of communication is achieved through ACK messages. In Z-wave architecture, controller manages slaves and maintain a routing table for entire network [23].

2.14 ZigBee

The ZigBee standard is specified by ZigBee Alliance which has adopted IEEE 8002.15.4 as its Physical Layer (PHY) and Medium Access Control (MAC) protocol. It is a wireless communication technology for low data rate limited range wireless networks. ZigBee compliant devices functions on 868 MHz, 915 MHz and 2.4 GHz frequencies allowing maximum data rate of 250 kbps [24]. This technology is mainly designed for battery powered devices having low data rate, low cost and need long battery life. Most of the time ZigBee devices remains in power saving mode i.e. sleep mode to conserve power thus creates ability to remain operational for longer duration. ZigBee stack has four levels, first two levels (PHY and MAC) are defined by IEEE 802.15.4 while remaining levels are specified by ZigBee Alliance.

2.15 Near Field Communication (NFC)

Near Field Communication (NFC) technology is jointly designed by Philips and Sony to allow short range communication among NFC enabled devices. NFC operates on 13.56 MHz frequency having communication range of about 10 cm, supporting data rates of 106 kbps, 212 kbps and 424 kbps [25]. NFC has three communication modes i.e. Read / Write mode, Tag Emulation mode and Peer to Peer mode. In read / write mode, NFC enabled devices can read or write to tags. In Tag Emulation mode, NFC enabled device act like tag or smart card for NFC readers. In Peer to Peer mode, two NFC devices are able to exchange data among themselves.

CHAPTER 3
IoT BUILDING BLOCKS

The goal of this chapter is to understand the requirements necessary to create IoT environment. Characteristics of IoT devices have been described to understand their key aspect. Various element of IoT architecture and components are explained needed for IoT operation. As IoT network has numerous devices with varying resources in terms of processing, power, memory and bandwidth capacity therefore categories of IoT devices is explained. Security is fundamental to IoT success, in this perspective different security requirement are described.

3.1 Introduction

Concept of IoT signifies a self-configuring, regulated and intricate network which enables wide range of things or devices such as RFID, sensors, tags and actuators to collaborate, interact and cooperate among themselves. The purpose of IoT is to interconnect variety of smart devices and form them as part of connected world [1]. WSN and M2M architecture is designed to perform prescribed task such as smart grid or home automation whereas IoT brings global connectivity and to direct them towards “anytime, anywhere and anyone” communications. Hence, when these smart devices are connected to Internet they turn out to be “Internet of Things”. IoT enables its consumers to access, interact and control their devices along with the data which has been uploaded on server or storage through connected devices on PAN, LAN, WAN or Internet. Moreover, smart devices communicate with each other employing various standards and protocols identical to that of web stack thus enabling devices to interact and collaborate over the Internet, so expanding their effectiveness and availability. The shared data or resources can be of sensitive in nature such as readings from sensor or medical appliance therefore meriting necessary precaution when transmitting or receiving data. Implementation of security mechanisms is challenging due to constrained resources in IoT [26].

In this chapter, various aspect of interconnected smart devices in IoT perspective have been identified and discussed which includes key qualities, architecture, key

components, services offered, categories of nodes and security requirements pertaining to IoT.

3.2 Characteristics of IoT

Following are the key features, qualities and characteristics of IoT: -

- **Heterogeneity**. IoT extends global connectivity for variety of devices in a network. These networks can be wired, wireless or cellular network containing diverse devices which are performing their prescribed operation.
- **Sensing Ability**. Objects in IoT have the ability to sense the environment for prescribed operation.
- **Addressing**. IoT employs standards and protocols for communication among entities which may involve unicast, multicast and broadcast communication. To communicate, objects have to have identity and addresses for interaction collaboration.
- **Autonomous Operation**. IoT network is capable of autonomous operation which includes configuration, processing and adjustment to dynamic environments.
- **Reliability**. Different protocols and mechanisms offer reliable performance and communication in IoT environment.
- **Secure Ecosystem**. IoT offers robust security environment to address challenges pertaining to privacy, confidentiality, integrity, network attacks and others. It is pertinent to mention that implementation of security mechanism and solutions poses significant challenges due to constrained resources in terms of computation, power, memory and bandwidth capacity.

3.3 IoT Architecture

IoT enables interconnectivity of huge number of heterogenous devices through Internet which mandates flexible architecture. There are various architectures proposed by academia and so far, they have not yet been merged to a reference model for manufacturers and IoT services providers [27]. Among available proposed architectures, three-layer model consists of application layer, network layer and perception layer [28] [29]. There are few other proposed models which add layers to IoT architecture [28] [30].

Keeping in view the proposed architectures, this section illustrates different elements as shown in figure 3.1 for implementation of IoT architecture.

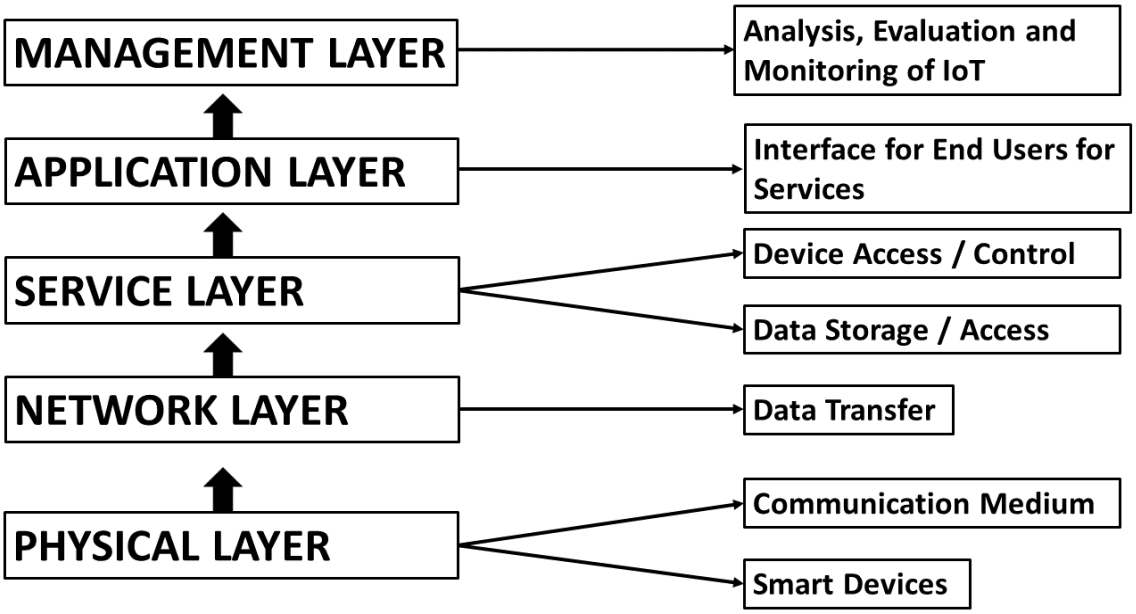

Figure – 3.1: IoT Architecture

- **Physical Layer**. This layer includes devices like sensors and actuators to perform functionalities such as sensing temperature and measuring weight, acceleration, humidity etc. As these devices are resource constrained in term of processing, power, memory and bandwidth therefore can carry out only given task and to connect with each other, with gateway or with Internet.
- **Network Layer**. Data collected by devices are required to be delivered for which networking and communication technologies enable interaction, collaboration and connectivity. Communication among devices can be achieved by employing various technologies such as ZigBee, Z-wave, BLE, WiFi, 3G/4G etc.
- **Service Layer**. At his layer, hardware and platforms in cloud over the Internet or data center offers ability to access and control the devices along with storage and access to data.
- **Application Layer**. This layer includes application software and interfaces for the end users to access IoT services. For example, measurements pertaining to temperature or humidity is provisioned to consumer who request for that measurement. This layer is important in terms of its ability to provide IoT services to its consumers.
- **Management Layer**. The most important layer which manages and ensure IoT system performances and related services. It involves processes to build

business model, design, analyze, implement, evaluate and monitor IoT ecosystem. In other words, management and monitoring of subordinate layer is attained by this layer.

3.4 Components of IoT Architecture

There are six major components as shown in figure 3.2 which are required to proffer functionalities. The components for IoT architecture includes identification, devices with sensing ability, communication technologies, processing, IoT services and power which are enlisted in table 3.1.

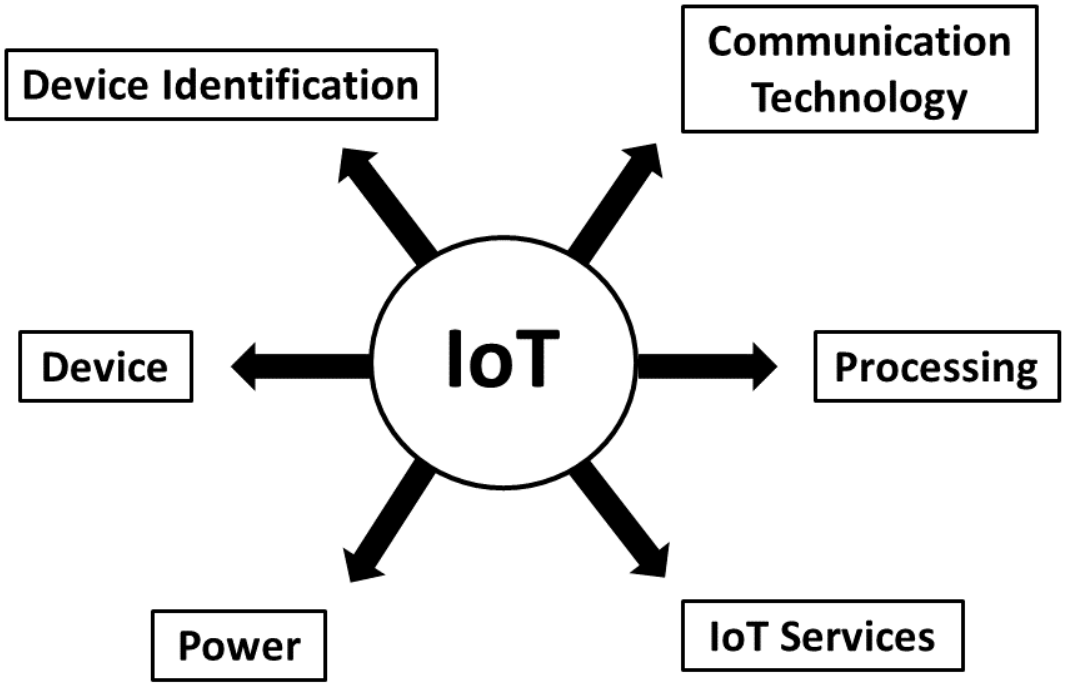

Figure – 3.2: Components of IoT Architecture

Table – 3.1: Summary of Components in IoT

IoT Components		Technologies / Applications
Device Identification	Device Name	Ubiquitous codes and Electronic Product Code
	Addressing	IPv4, IPv6 and 6LoWPAN
Devices		Actuator, embedded sensors, wearable health devices, tags etc.
Communication Technology		Z-wave, ZigBee, BLE, WiFi, IEEE 802.15.4, NFC, 3G/4G etc.
Processing	Software	Contiki, TinyOS, LiteOS, RiotOS etc.
	Hardware	Arduino, Raspberry PI, Gadgeteer etc.
IoT Services		Identity Related Services, Ubiquitous Services, Collaborative Aware Services and Information Aggregation Services
Power		To last for longer duration

- **Device Identification**. Naming the device and its addressing cerates devices identification. Device name provides identity e.g. “Tempo” for temperature sensor installed at home whereas addressing (IPv4, IPv6) is related to network for communication e.g. IP address of “Tempo” is 192.168.1.1. Various identification mechanisms exist for IoT devices such as Ubiquitous codes and Electronic Product Code. Moreover, addressing scheme for interconnected devices includes IPv4 or IPv6. It is highlighted that device name is not unique globally therefore addressing in terms of IPV4 or IPv6 is available to exclusively identify the device in communication networks. For IoT, 6LoWPAN offers compression methodology for traditional IPv6 standard that allows IPv6 addressing in IoT ecosystem.
- **Devices**. Various devices with defined functionality forms part of IoT for required services. In this regard, sensing is the process of detecting the environment or ability to measure the event and then directing collected data to server or cloud. Collected data is then processed and analyzed for prescribed operation or functionality. Hubs, gateways and application software allows consumer to extract data, access and control devices / appliances installed within building. Furthermore, single board computers (SBCs) such as Arduino, Raspberry PI etc with sensing ability and other functionalities are utilized for IoT product. These devices are normally

connected to central entities for requisite services and management reasons.

- **Communication Technologies**. Connectivity within the network or among other networks materialized the concept of IoT. Communication technologies creates connectivity among heterogenous devices in order to proffer specified services. Technologies such as Z-wave, ZigBee, BLE, WiFi, IEEE 802.15.4, NFC and others can be employed for communication among devices.
- **Processing**. IoT devices with unique identity, interact and collaborate with each other by employing preferred communication technology for requisite services. In this context, central units within the network act as "Central Intelligence" of IoT. Different hardware platforms have been designed to run IoT such as Arduino, Raspberry PI, Gadgeteer etc. Furthermore, various lightweight operating systems as given in table 3.2 are also designed and available for IoT such as Contiki, TinyOS, LiteOS and others [31,32,33,34]. Requisite hardware and software; combines and produce processing for required IoT services. Moreover, cloud computing and their offered platforms also provide computational ability for IoT related services where devices send collected data to cloud which is then processed in real time for customer or users.

Table – 3.2: Lightweight OS

Light Weight OS	Language	Memory Usage in Kb
RiotOS	C/C++	1.5
TinyOS	nesC	1
LiteOS	C	4
Contiki	C	2

- **IoT Services**. The services which are offered by IoT paradigm can be categorize under four classes [35] such as Identity Related Services, Ubiquitous Services, Collaborative Aware Services and Information Aggregation Services. Identity related services are used in shipping industry, transportation and others for identification purposes. Information Aggregation services gathers data for end users when requested. Collaborative aware services are used to attain data for processing and

taking decisions accordingly. The ultimate goal of IoT is to combine above mentioned services and offer Ubiquitous services to offer real time services "at any time, to anyone and anywhere" e.g. Smart Cities.

- **Power**. IoT devices such as actuators, sensors, gateways and other requires energy to operate for specified task. Hardware and software platforms along with other mechanisms needs to be designed in a manner that device must consume less power and last for longer duration.

3.5 Categorization of Constrained IoT Devices

Individual IoT device is resource constrained in terms of processing, memory, power and bandwidth. These resources which in IoT ecosystem allows daily life objects to grow into smart and intelligent by using embedded sensors or actuators. These interconnected smart devices exhibit constraints in following manner: -

- **Computation Power**. Processor in actuators and sensors are not as much powerful as are found in laptops, computers, tablets and other devices. As, IoT devices have to perform specified task therefore computational power is not kept large. Secondly, increasing processing capability amplifies the cost as well which is not suitable for developer and manufacturers. It is because of limited computational power; implementation of communication protocols and security solutions requires deliberation according to on board processing capability.
- **Memory**. Memory in terms of volatile and nonvolatile (RAM and ROM) in IoT devices are limited. Flash memory is utilized for storage of data and application software whereas RAM is used as temporary memory for computational purposes. However, with technological advancement memory has been improved in term of size and capacity but still cannot meet the requirement of many algorithm in IoT.
- **Energy Requirement**. For requisite operation, power is crucial for any electrical device. In IoT ecosystem, power consumption is related to communication and processing requirements. Larger the communication range, power output and data rate; greater will be the overhead on power requirement. Similarly, increase in computational capability will also increase energy needs.
- **Bandwidth**. Increase in bandwidth means more processing and power consumption. Therefore, communication range, data rate and selection of

frequency merits careful study of available resources i.e. computation and battery life.

Diverse range of constrained devices with different resources are becoming part of IoT environment which includes personal devices, automation system, WSN, M2M, embedded sensors and others. In this context, IETF proposed classification of resource constrained devices is based on ROM and RAM size [36]. Proposed classification comprises of three categories of constrained devices i.e. Class 0, Class 1 and Class 2 devices as enlisted in table 3.3. Brief description of each category is as under: -

Table – 3.3: Categories of IoT Devices

Device Category	RAM Size in Kbytes	ROM Size in Kbytes
Class 0	Less than 10	Less than 100
Class 1	10	100
Class 2	50	250

- **Class 0 Device**. These devices are extremely constrained having RAM size less than 10 Kbyte and ROM size less than 100 Kbytes. Due to limited resources, these devices do not support complex security mechanisms and solutions.
- **Class 1 Device**. These devices are slightly better than Class 0 devices. Class 1 devices have RAM size of 10 Kbytes and ROM size of 100 Kbytes. As appropriate RAM/ROM is available therefore these devices are capable to contribute in Internet communication and support lightweight security solutions.
- **Class 2 Device**. These devices have RAM size of 50 Kbytes and ROM size of 250 Kbytes therefore can support variety of protocols and security mechanisms.

3.6 Security Requirement in IoT Devices

Objective of security mechanism in IoT ecosystem is to safeguard data, resources and privacy from adversaries [37]. Major security requirements in IoT includes: -

- **Confidentiality**. It is defined as the “protection of data from discloser to unauthorized person, party or systems”.
- **Integrity**. It is a methodology to avoid modification of data by unauthorized entity.

- **Authentication**. This process involves verifying the identity of a person or system accessing the resources, data or device.
- **Authorization**. This process is based on effective authentication and identity management which ensures that the authorized entity is involved with defined rights to access IoT resources.
- **Availability**. It is the methodology or mechanism through which resources remains available to authorize entity.
- **Non-Repudiation**. It is process in which an entity is unable to deny about the transmission which it has generated earlier.

CHAPTER 4
DEPLOYMENT STRATEGY OF IoT

The goal of this chapter is to explain deployment strategy pertaining to IoT devices in a network. IoT services can be provisioned in several ways where centralized and distributed approach can be adopted. Each approach has its own vital issues and security challenges which are described to understand the practicality and applicability in real world. It is necessary to understand features, major principles including advantages and disadvantages of each approach, therefore discussed in succeeding sections. Security analysis related to both the approaches have also been carried out to identify true challenges. Mainly, the purpose of this chapter is to assess centralized and distributed approach pertaining to IoT network.

4.1 Introduction

The concept of Internet of Things (IoT) can be summarized as "the network of interconnected smart entities". These heterogeneous entities can be appliances, cars, computers, mobiles, tablets, lights and various other things which have their prescribed functionalities in a network to offer services at any time and at any place [38]. It is the end user that is "human" which is the prime beneficiary of this technology. Various technologies act as building block to IoT, which involves wireless sensor networks (WSN), cloud services, radio frequency identification (RFID), machine to machine (M2M), so on and so forth [39]. In addition, IoT has variety of operational spheres such as automotive, agriculture, military, logistics, healthcare and numerous other fields.

Diverse approaches can be utilized in order to implement the vision of IoT for provisioning of several services [40]. Primarily, centralized and distributed approach can be implemented to deploy IoT devices in a network [41]. Centralized approach, which is basically client / server architecture where central entity with which IoT devices are connected and there is not much support to directly access IoT entity. Cloud services are the practical manifestation of centralized methodology where application software are located over the Internet connected with IoT entities at some other location thereby rendering services to end user. Likewise, the devices in central approach can exchange intelligence with other IoT network and creates new enriched services [41], [42]. For example, IoT devices of different cities can exchange atmospheric data and creates

complete atmospheric picture for entire country. Alternatively, in a distributed or decentralized approach, collected data and related services are offered from the edge of the network where various devices and applications in a network collaborate with each other dynamically. If required, smart objects in distribute approach interact and communicate with backend services located over the Internet without a central device [41], [43]. Both the approaches have different feature and advantages which are analyzed in succeeding section.

4.2 Centralized Methodology for IoT Deployment

In this scenario, the functionality of entities such as sensors, mobiles, lights, locks and others in a network is to collect data or to act on received instructions which is only be coordinated through single central unit. In other words, devices in a network performs prescribed operation through central unit and do not accept connection other than central unit. The collected data is processed by central entity and provided to end user. Accordingly, if the consumer chooses to use IoT services or chooses to access device in a network; first the connection is made with central device from where user interact with smart devices through interface delivered by central unit. This central entity can be a server, hub, gateway, cloud or anything which controls the connections from inside to outside and from outside to inside the network [41]. To understand the application of this approach, analysis of various aspect has been carried out which includes the impact and security analysis. Based on these analysis, advantages and disadvantages are also drawn.

The central entity is computational device with considerable resources to handle traditional computing and security protocols. In terms of security, central entity provides extra layer of security where Internet and IoT network is separated by a check point for inbound and outbound traffic. Figure 4.1 shows the layout of centralized deployment.

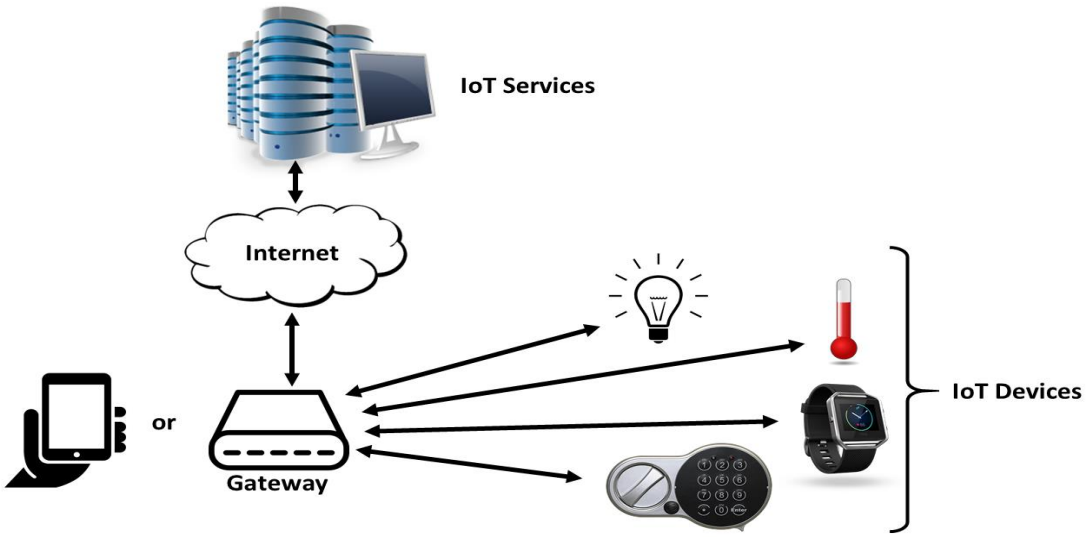

Figure – 4.1: Centralized IoT Approach

4.2.1 Impact Analysis of Centralized IoT Network

In this section, analysis of centralized approach has been carried out to assess following features: -

4.2.1.1 Collaborative Access

For the growth of business and enriched IoT services for end users, exchange of data is an important factor. To accomplish this, entities must interact and access each other and permit to collaborate. In centralized approach the raw, preprocessed and processed data is exchanged among parties and vendors. The central device provides visibility and control to owner over data selection for sharing with other entities while restricting sensitive data. For such collaboration, APIs for acquisition and provisioning of data are required for which programmers will develop APIs and other IoT application giving boost to software development business including investment in IoT sector.

4.2.1.2 Interoperability

IoT is characterized by its heterogeneous nature, where various components must be able to operate with different protocols and standards to offer required services. With the introduction of APIs and other interfaces within single central entity, the devices can be made to communicate with each other as all the devices are connected to central unit.

4.2.1.3 Consistency

IoT architecture is required to perform prescribed operation for necessary services, thus assurance pertaining to availability and reliability is an important feature. Centralized approach provides a single point from where all connected components can be managed and monitored for stipulated functionality. However, centralized approach is a single point of failure due to which complete network will become redundant on occurrence of any fault.

4.2.1.4 Data Management

Various components in IoT network generate data either by sensing or processing therefore data management is of prime importance. In centralized approach, single central device provides the control over the data in terms of sharing, its access, security and storage.

4.2.1.5 Workload Management

Deployed IoT network will not remain as it is, various devices will add to it from time to time. Collection, generation and processing of data will increase exponentially thus level of performance and extensibility is an important consideration. A central device can be configured and upgraded to handle extra workload to add additional smart devices.

4.2.1.6 Fault Tolerance

Devices in IoT network are expected to perform their specified functionality. Devices can either malfunction or start offering false data on occurrence of any fault which can become nightmare for end users. In centralized IoT deployment, discovery of fault is straightforward as the complete network is visible to single central device. Monitoring of components through central device is easy and any inconsistency can be traced thus enable timely troubleshooting including replacement.

4.2.1.7 Implementation of Security Mechanism

Security can be managed through single central device with which all the other components are connected. Requisite security mechanism can be implemented or installed on central device from where security parameter can be configured, controlled and monitored. The secure parameters may include security of communication channel, sharing of data, access policies, authentication mechanism and fault tolerance. It is highlighted that security mechanism are on central device therefore it also becomes the prime target for adversary. Thus, security of central device itself is also important.

4.2.2 Security Analysis of Centralized IoT Network

IoT is collection of smart devices in a network which interact with each other and in future this number will grow to billions of devices all around the world. In this context, security is one of the key challenges which needs to be addressed for the success of IoT. It is therefore imperative that interactions, devices itself and networks must be protected along with restricting the incidents which can cause harm to IoT. The amount of attack vectors available to adversaries is also growing as compared to present day connectivity mainly due to increase in connected devices. In this section analysis of security concerns has been carried out to assess the effectiveness of centralized approach.

4.2.2.1 Identity and Authentication Mechanism

The foremost element is to identify and authenticate an entity into a network without which desired services cannot be made available or the adversary can incorporate himself as trusted entity. In centralized approach, this issue is simple to handle due to presence of single central device with which other smart devices are connected. Specifically, effective identity and authentication mechanism can be installed in a central entity to offer better control and to create limited set of entry points into the network. Each time a new device attempt to access the network, it has to authenticate itself to single central device before accessing the network.

4.2.2.2 Access Control Mechanism

Like, identity and authentication; the access control mechanism is also simple to implement due to single central entity. Access control rights can be configured in central device from where access to legitimate entities is granted to access required

resources. As access right are configured in single device therefore simplicity and better control is involved in implementation and management.

4.2.2.3 Network Security Mechanism

IoT devices are constrained in terms of processing capability, power availability, memory and bandwidth. Standard security protocols or traditional enterprise security solutions requires considerable computing resources therefore difficult to implement in constrained IoT environment. Security challenges such as negotiating of security algorithms and selection of protocols requires deliberation in implementation in constrained environment. Criticality of data, amount of data, accessibility to network, integrity requirement and number of security protocols must be considered for implementation of security mechanism in resource constrained devices.

In case of centralized approach, the single central device is efficient in terms of processing, power, memory and bandwidth to implement security mechanisms. Moreover, upgrading and patching of network security mechanism is also manageable due to availability of resources in single central device.

4.2.2.4 Device Security

Smart devices in IoT network has to perform its prescribed functionality which includes, collection of data, processing if required, interact with other entities, data storage and perform stipulated operation. All this functionality requires well managed processing, power, memory and bandwidth. Adversary will attempt to manipulate the device operation or corrupt it to not perform its prescribed functionality. Device security requires processing and memory to carryout security operation. Addition of security mechanism to normal operation can create extra load on processing and memory. In this context, hardware and software specification merits careful deliberation and analysis to balance out both normal operation and security requirement.

In centralized approach, heavy processing and large data storage are delegated to single central unit which conserve processing and memory in constrained devices for security mechanism. This leverage is one of the prime trademark of centralized approach where security mechanism can be hosted without affecting normal operation of smart devices in a network.

4.2.2.5 Privacy

Entire IoT network is controlled by single central device thus empowering the owner to decide and implement privacy policies whether to share data or not with a particular entity. Another aspect of privacy in IoT is the tracking and profiling of users without their consent. Again, this profiling and tracking can be controlled by implementing policies in single central device.

4.2.2.6 Data Security Mechanism

Security of data either stored or in transit is one of the prime security concern. In IoT architecture, security of data can be achieved by using cryptographic algorithm. In this regard, a significant decision is involved whether to use symmetric encryption or asymmetric encryption. Secondly, key management is another factor which needs optimal handling in establishing data security. It is highlighted that encryption itself consumes high processing resources especially asymmetric encryption. Light weight encryption algorithms like RECTAGLE, BLAKE, DTLS etc are the solution for constrained environment which consume less processing power. In centralized approach, the central entity has sufficient processing capability and memory to employ required encryption mechanism. So, asymmetric encryption can be used for the services or data when using web applications. On the other hand, symmetric encryption which consume less resources can be used between central entity and constrained devices. However, symmetric encryption requires effective key management because loss of key can compromise the entire security.

4.2.3 Advantages of Centralized IoT Network

Based on the above analysis, advantages of centralized approach of IoT network are, but not limited to following: -

- Network and system administrator can efficiently access the devices in a network. End user in a smart home can also have better access to devices by having user friendly interface.
- Resources pertaining to network can be managed efficiently and effectively.
- Efficient security can be achieved by introducing security measure in central entity which may include firewall, IDS/IPS, antivirus, encryption, ACL and others.
- Better control over configuration management.
- Act as barricade against the attacks coming from Internet.
- Patch management is efficient as one central entity is patched and other components are patched securely through central device.
- Inclusion of additional hardware is single central device is easy in order to handle extra workload
- Ability to track communication status with components in a network.
- Ability to collaborate other networks for exchange of data and information.
- Centralized approach can be a preferred option for organizations, companies and consumers which are concerned about security of data. This approach provides considerable control over complete network devices to monitor and manage the assets. So, vendors offering IoT services based on centralized

approach have good prospects to do business in the market. Already, many vendors are offering IoT services which is based on centralized approach.

4.2.4 Disadvantages of Centralized IoT Network

Centralized methodology is an endeavor to achieve better management, but it also has integral shortcomings which are listed below: -

- Adversaries strive for the target which offer immense benefit and central entity appears in this category.
- Central device can have suitable protection arrangements but any vulnerability can jeopardize the whole system or network.
- User involvement is another factor which can create misconfiguration due to limited expertise and yielding an opening for attackers to exploit the network.
- Centralized approached is a single point of failure as downtime, interruption, fault or malfunction of single device can cause damage to entire network.
- Adversary can also capture processed data, instead of raw data from a single entity.

4.3 Distributed or Decentralized Methodology for IoT Deployment

In distributed approach, devices within the network operate autonomously and collaborate with each other. Moreover, information and delivery of services are located at the edge of network as shown in figure 4.2. In other words, this system involves several objects that form a network to interact with each other and emerge to end user as distinct coherent structure. Distributed approach empowers the devices in a network to gather, process, merge, and deliver information including services to other entities without depending on a totally centralized arrangement [41], [44], [45].

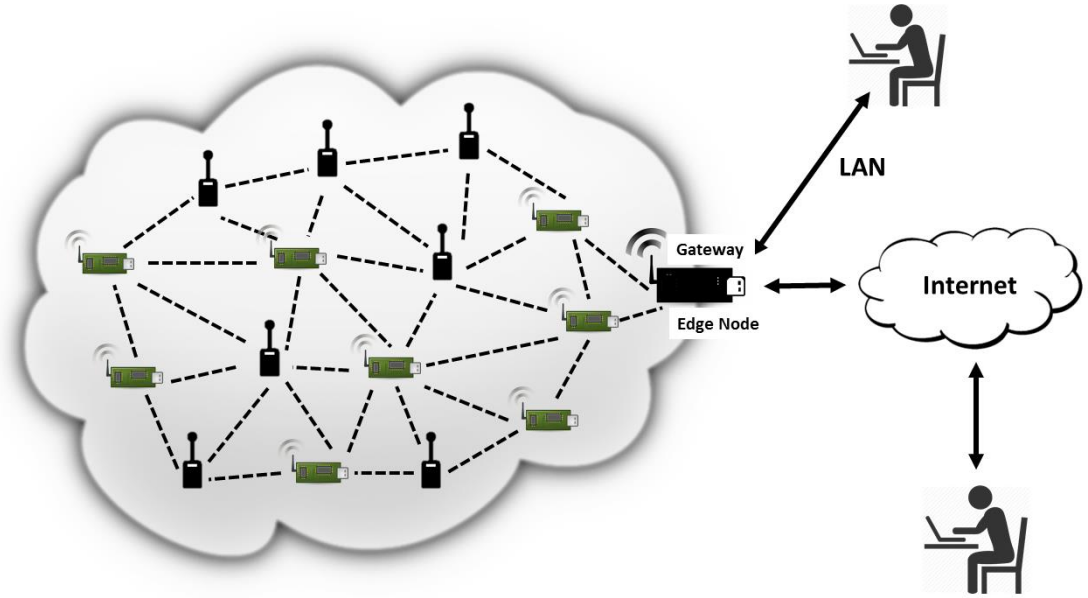

Figure – 4.2: Distributed IoT Approach

4.3.1 Impact Analysis of Distributed IoT Network

To understand the benefits of this approach, various aspects have been analyzed by using following conditions and features: -

4.3.1.1 Collaborative Access

The collected data is accessible to other entities and vendor for usage through edge devices in a network. In this approach, devices of several vendors may be operating and performing particular functionalities therefore collaboration with 3rd parties are beneficial. Various service providers can collaborate to offer enriched services to end user. Such collaboration and exchange of information can facilitate in business growth including investment in technology.

4.3.1.2 Interoperability

In centralized methodology, achieving interoperability is simple by introducing APIs, application software and requisite hardware in a central entity. On the other hand, interoperability is complex in distributed approach where each of the different device is required to be configured for interaction.

4.3.1.3 Consistency

IoT architecture is expected to execute prescribed function for mandatory services. Distributed approach provides high assurance pertaining to availability and reliability. In case of any malfunction in a device then other devices are available and can continue to perform their operation, thus, causing only local data loss and partial failure.

4.3.1.4 Data Management

"Pull and Push" methodology can be adopted in distributed approach for data management. In other words, data can be provisioned when needed or retrieved when required. However, compared to centralized approach the data management is challenging as many entities are involved in data handling.

4.3.1.5 Workload Management

Various smart devices operate coherently in a network, therefore, facilitates management of computational and data resources.

4.3.1.6 Security Management

Decentralized and heterogeneous nature of distributed approach creates complexities in implementation of security mechanism. As each device is autonomous in a network therefore needs to be secured independently after necessary evaluation of available processing, power, memory and bandwidth.

4.3.1.7 Fault Tolerance

Inconsistent security mechanism can jeopardize sensitive data and privacy. In distributed IoT deployment, fault discovery methodology can be implemented in order to identify faults and if possible assigning task to other device for services. It must be noted that discovery mechanism can be an added feature in a device for which processing, power and memory needs to be managed.

4.3.2 Security Analysis of Distributed IoT Network

In distributed deployment of IoT, the devices not only interact with each other but users can also access each device for local data or services. Due to dynamic nature of distributed approach, each device needs to be secured separately. Security implementation on each of the device requires careful evaluation of constraints such as processing, power, memory and bandwidth which are inherent to IoT device. The adversary can control part of the network or few devices but due to distributed nature of network, it is difficult to bring down the entire network. There are wide range of security challenges to distributed IoT, analysis of few are as under: -

4.3.2.1 Identity and Authentication Mechanism

This feature is bit complex in distributed approach as compared to centralized methodology of IoT network. In distributed architecture, devices interact with each other and provide data through edge devices while user can also access the objects within the network for local data. Therefore, identity and authentication mechanism needs to be implemented on every device and requires deliberate efforts to generate trust within the network.

4.3.2.2 Access Control Mechanism

In distributed IoT deployment, the challenges of access control are same as of identity and authentication mechanism. Wide variety of devices in distributed network are operating autonomously therefore create complications in access control policies. Each device or group of devices in distributed approach needs to be configured separately for access policies which may be based on access control list (ACLs), role base access control (RBAC) mechanism etc. This separate configuration of devices also creates management problems which needs effective management schemes to achieve efficiency.

4.3.2.3 Network Security Mechanism

Processing, power, memory and bandwidth merits efficient management in IoT ecosystem and their availability is limited as compared to traditional computing devices. In this context, standard network security mechanisms and protocols are difficult to apply in constrained devices. Selection of security parameters, algorithms and protection mechanisms necessitate evaluation, as each of the procedure has its own processing overhead including power and memory. In distributed approach, each device in a network needs to be configured separately according to task and functionality of the device. Moreover, patching and updating the network security mechanism is also challenging due to open interaction of devices.

4.3.2.4 Device Security

In distributed IoT, security of device itself is important because collection of data and processing is carried out by each device. Securing each device needs careful planning and monitoring, any bug or vulnerability left can compromise the device. Moreover, security audit of distributed approach is also complex in terms of time and large number of devices in a network. Securing each device is challenging due to non-availability of single interface for number of devices and also creates complexity in their security audit. In distributed approach for IoT, tradeoff will always remain between normal functionality and security mechanism. Design consideration is another element which dictates security mechanism and its intended services.

4.3.2.5 Privacy

Absence of central controlling unit make privacy challenging and creates complication for distributed IoT. Each device in distributed approach is required to be design and configured keeping in view processing capability and memory. Additional privacy mechanism will become processing overhead where device has also to perform its stipulated functionality.

4.3.2.6 Data Security Mechanism

Processing overhead of asymmetric encryption is more compared to symmetric encryption. As symmetric encryption requires less processing overhead

therefore preferred scheme for constrained IoT devices. In symmetric encryption, key management has a pivotal role for security of data. In symmetric encryption, if key is compromised then entire data security mechanism is lost. In distributed approach, key establishment is very challenging due to large number of devices and non-availability of single interface to interact with each of the device.

4.3.3 Advantages of Distributed IoT Network

Collaboration among smart devices and with other entities in distributed approach has advantages, which are as under: -

- Dynamic discovery permits easier inclusion of new devices in a network, without disturbing operational status.
- Distributed approach offers redundancy as other devices will continue to perform their prescribed operation in case of any failure in one device.
- There is no single point of failure in distributed approach as compared to centralized methodology of IoT.
- Sharing of data among the devices in a network provides ability to retain some control over the data which is stored locally.
- Better suited approach for large networks.
- Distributed IoT methodology is somewhat similar to hybrid cloud infrastructure. Various entities from different vendors are functional in a network and offering particular services to customers. Complexity is involved in merging divergent device with different protocols for which variety of APIs and application software are required.

4.3.4 Disadvantages of Distributed IoT Network

Distributed approach has its own limitations, which are as under: -

- The decentralized nature of this approach creates difficulty in administration.
- Implementation of security mechanism in distributed approach is complex.
- Data recovery mechanism or to back up the data requires variety of procedure which is to be implement on different devices in a network.
- Patch management and updating firmware is complex.
- Bugs in software are difficult to trace.
- Interoperability is also a complex feature to achieve in distributed approach.

4.4 Comparison between Centralized and Distributed IoT deployment

Features	Centralized IoT	Distributed IoT
Collaborative Access	Available through single central entity	Multiple devices in network are accessible
Interoperability	Simple due to central device	Complex due to existence of many devices in a network
Consistency	Single point of failure	Network continue to work in case of any device failure
Data Management	Effective and efficient data management	Pull and push methodology provides data management
Workload Management	Provides required level of performance and extensibility	Required performance and extensibility available
Security Management	Security in entire network through central entity	Each device is required to be configured separately
Identity and Authentication	Device to single central entity, Easier to implement	Device to device, Challenging
Access Control	Managed through single central entity, Simple to implement	Varies according to type of devices and data, Require thorough management
Network Security	Governed through single central device, Better control and management	Varies from device to device, Requires detail analysis
Device Security	Processing and storage of collected data at central device, Conserving resources in device for security	Thorough workout required to balance security and normal functions, Additional silicon area required for security mechanism
Privacy	Control lies with central device	Devices needs to be configured separately
Fault Tolerance	Monitoring and detection of fault through central entity	Specialized discovery mechanism needed to trace and monitor each device
Data Security	Effective encryption key management	Deliberation required for key management

CHAPTER 5

PROTOCOLS FOR IoT ARCHITECTURE AND SECURITY ANALYSIS

There are various protocols and communication technologies are available for IoT. In this chapter, different protocols and communication technologies have been described. Among many, protocols such as IEEE 802.15.4, 6LoWPAN, RPL and CoAP in IoT has been explained in detail. Focus has been given to security offered by these protocols with a view to carry out their security analysis.

5.1 Introduction

IoT is the evolution of Internet where smart devices not only interact with each other but also connected to end users and related devices through Internet. IoT materializes vision of ever evolving Internet where entity holding computational power is capable to communicate with devices utilizing protocols and communication technologies [2]. The developing notion of IoT is swiftly discovering its direction in our lives with the aim to enhance quality of life by connecting smart devices. Generally, IoT is enabling factor of autonomous operation of technologies all around us such as street lights, locks, transportation and many others. In these frameworks; various standards, protocols and technologies are the building blocks to deliver functionality of IoT. Many of IoT applications are supposed to engage huge quantity of smart interconnected smart devices therefore cost is an imperative factor. Cost limitation and demand for economical IoT applications creates constraints in terms of processing, memory, power and bandwidth in smart devices [36]. This constrained ecosystem is the motivational factor to designed optimized protocols, communication technologies and security solutions capable of offering reliable and efficient functionality. Many of the standards, protocols and communication technologies have been proposed and specified in the realm of IoT to bring reliable, efficient, secure and cost effective operational mechanism.

In this chapter, concise attributes of different protocol stack and communication technologies have been stated in section 5.2. However, security offered by protocols such

as IEEE 802.15.4, 6LoWPAN, RPL and CoAP in IoT architectures as shown in Table 5.1 have been discussed in detail with a view to carry out security analysis of said protocols. It is expected that security analysis of said protocols will contribute towards research community interested to optimize, improve or develop new solutions to address security concerns in IoT. Brief overview of discussed protocols is as under: -

- **IEEE 802.15.4**. Connectivity at Physical (PHY) and Medium Access Control (MAC) layers are specified in IEEE 802.15.4 which mandates 128 bytes of packet for transmission at higher layers [14], [15].
- **6LoWPAN**. IPv6 mandates Maximum Transmission Unit (MTU) size of 1280 bytes which is larger than MTU size (128 bytes) specified by IEEE 802.15.4. This requires optimization which has been provided by IPv6 Low Power Wireless Personal Area Network (6LoWPAN) by header compression and packet fragmentation [16].
- **RPL**. To manage large number of fragmented packet and handle routing in constrained environment, Routing over Low Power and Lossy Network (RPL) provides mechanism for fragmented packets and their reassembly [17].
- **CoAP**. Constrained Application Protocol (CoAP) is an application layer protocol designed only for UDP over 6LoWPAN. CoAP allows end to end communication among constrained devices [18] [19]. For translation of CoAP to HTTP or vice versa, gateway is used in a network.

Table – 5.1: IoT Protocol at Different Layers

OSI Layer	IoT Protocols	Traditional Computing Protocols
Application Layer	CoAP	HTTP
Network Layer	RPL	IPv4, IPv6
	6LoWPAN	
Link Layer	IEEE 802.15.4	IEEE 802.3, IEEE 802.11

5.2 Protocol Stack and Communication Technologies for IoT

Various protocols and technologies have been designed to meet crucial conditions such as computational efficiency, power efficacy, reliability and Internet connectivity among constrained smart devices; thus, creating a platform for new services and applications. In this regard, Table 5.2 illustrates only a few of protocols and communication technologies pertaining to IoT: -

Table – 5.2: Major Protocols and Communication Technologies for IoT

Domain	Protocols	Brief Detail
Identification Mechanism	Electronic Product Code (EPC)	A universal identifier which provides unique identity to smart devices [46].
	uCode	uCode mechanism is considered as building block of IoT which is an identification number system to identify IoT objects [47].
Communication Technology	WiFi	It is based on IEEE 802.11 standard for wireless connectivity employing 2.4 GHz or 5 GHz frequency [20].
	Bluetooth Low Energy (BLE)	It utilizes short range radio with minimum power output to operate for longer duration [21], [22].
	Z-Wave	It is a low power wireless communication technology designed to be used in home automation and small size commercial units. Coverage range of Z-wave is about 30 meters and is designed for devices to transmit less data such as fire detectors, ambient control, HVAC systems, access control devices and others. Data rate is 40 kbps in Z-wave which functions in ISM band using 900 MHz frequency [23].
	ZigBee	ZigBee is specified by ZigBee Alliance which has adopted IEEE 8002.15.4 as its Physical Layer (PHY) and Medium Access Control (MAC) protocol. ZigBee compliant devices functions on 868 MHz, 915 MHz and 2.4 GHz frequencies allowing maximum data rate of 250 kbps. This technology is mainly designed for battery powered devices having low data rate, low cost and requiring long battery life [24], [48].
	Near Field Communication (NFC)	NFC operates on 13.56 MHz frequency having communication range of about 10 cm supporting data rates of 106 kbps, 212 kbps and 424 kbps. NFC has three communication modes i.e. Read / Write mode, Tag Emulation mode and Peer to Peer mode [25].
Infrastructure	IEEE 802.15.4	This protocol was designed to specify Medium Access Control (MAC) and Physical Layer (PHY) communication for low rate wireless personal

Domain	Protocols	Brief Detail
		area network (LR-WPAN). It creates specification for low data rate, low cost, low power consumption and high through put therefore used by WSN, M2M and IoT [14], [15].
	IPv6 Low Power Wireless Personal Area Network (6LoWPAN)	6LoWPAN offers methodology of mapping between traditional IP networks and IEEE 802.15.4 based network by means of header compression and fragmentation [16].
	Routing Protocol for Lower Power and Lossy Network (RPL)	RPL is specified by Internet Engineering Task Force (IETF) to support routing needs for simple and complex traffic models like multipoint to point, point to point and point to multipoint [17].
	Nano IP	It stands for Nano Internet Protocol designed with minimal overhead to create connectivity for constrained IoT devices [11].
Transport Layer Protocols	User Datagram Protocol (UDP)	UDP is preferred protocol for IoT in transport layer as it is connectionless protocol and do not puts constraint on limited resources [18], [19].
	Datagram Transport Layer Security (DTLS)	DTLS is based on TLS which provides equivalent security measures like confidentiality, authentication and integrity. DTLS mechanism consist of initial authentication of devices, key agreement and finally protection of data through secure channel [18], [19].
	Quick UDP Internet Connection (QUIC)	QUIC connect two devices over UDP with less transport latency. Moreover, bandwidth estimation is also carried out to avoid congestion [49].
Application Layer	Constrained Application Protocol (CoAP)	CoAP utilizes set of techniques to compress application layer protocol metadata without conceding application interoperability by using representational state transfer (REST) architecture [18], [19].
	Message Queuing Telemetry Transport (MQTT)	MQTT is specified for connections where “small code footprint” is required and bandwidth is limited [50].

Domain	Protocols	Brief Detail
	Advanced Message Queuing Protocol (AMQP)	AMQP is designed and specified for connection among servers deployed for IoT objects [50].
	Web Socket	It is a bi-directional communication mechanism between client and server. This standard removes majority of complexities in full duplex web connectivity [50].
	Data Distribution Service for Real Time System (DDS)	DDS is high performance compatible exchange of data using "publish-subscribe pattern". It can be used in applications such as e-health devices, transportation system and others [51].
Others	uIP	It is an open source TCP/IP stack which can be used for 8 bit or 16 bit controllers developed by Swedish Institute of Computer Science [52], [53].
	Time Synchronized Mesh Protocol (TSMP)	TSMP is for self-organizing wireless devices where communication among devices is carried out in allotted time slot [54], [55].
	Wireless HART	This technology is based on "Highway Addressable Transducer Protocol" for connectivity among wireless devices using 2.4 GHz in Industrial, Scientific and Medical (ISM) band and IEEE 802.15.4 protocol [56].

5.3 IEEE 802.15.4

This standard has been specified with a view to support low energy connectivity at MAC and PHY layer. IEEE 802.15.4 specifies data rate of 250 kbps in approximately 10 meters of communication range.

5.3.1 Connectivity at PHY Layer

PHY layer handles smart devices in terms of transceiver, selection of channel and management of signals. Salient are as under: -

- This standard specifies use of 2.4 GHz in ISM band with 16 channels.
- To achieve reliability and avoid interference, this standard employs Direct Spread Spectrum (DSS), Chirp Spread Spectrum (CSS) and Direct Sequence Ultra Wideband (UWB) modulation mechanism.

- Size of data frame at this layer is 128 bytes so as to avoid errors in low energy and lossy wireless connectivity.

5.3.2 Connectivity at MAC Layer

This layer carries out management of beaconing, access to physical channel, frame validation, allocation of time slots, association of nodes and security. Devices can be identified by utilizing 64 bit or 15 bit identifiers. As far as collision avoidance is concerned, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is employed. Detail of device types and frame types at this layer are: -

- **Device Types**. There are two types of devices namely "Full Functional Devices (FFD)" and "Reduced Functional Devices (RFD)". FFD is capable to manage devices in a network whereas RFD only carries out communication with other devices. Based on FFD and RFD, different networking topologies can be employed such as peer to peer, star and cluster network.
- **Frame Types**. There are four types of frames namely data frame, acknowledgement frame, beacon frame and MAC frame.

5.3.3 Security Services by IEEE 802.15.4

Security is offered only at MAC layer by using Advanced Encryption Standard (AES). Detail of security services offered are proffered below: -

5.3.3.1 AES Security Modes

IEEE 802.15.4 provides different security modes at MAC layer and these modes offer various security solutions in terms of confidentiality, authentication and integrity as illustrated in Table 5.3.

Table – 5.3: AES Security Modes

Security Modes	Offered Security
AES-CCM (Cipher Counter Mode)	• Confidentiality by encryption of data. • Authentication service.
AES-CBC-MAC (Cipher Block Chaining Mode and Message Authentication Code)	• Authentication Service. • Integrity Service • No confidentiality protection.
AES-CTR (Counter Mode)	• Confidentiality by data encryption. • No Authentication.
No Security	• No Confidentiality. • No Authentication.

- Protected data frame is shown in figure 5.1 where secured frame is identified by a bit at the beginning of packet header called “Frame Control”.
- When security is applied “Auxiliary Security Header” is added which consist of fields i.e. Security Control, Frame Counter, and Key Identifier.
- The “Security Control” consist of three fields namely Security Level, Key Id Mode and Reserve field. Security Level field, specifies the selected AES modes as mentioned in Table 5.3.
- This standard mandates the use of 128-bit key which is known to parties involved in secure communication or can be determined by “Key Identifier Field” which consist of “Key Source and Key Identifier”.
- **Confidentiality**. For data encryption, data is encrypted in AES using counter mode (CTR) with 128-bit key.
- **Integrity and Authenticity of Data**. AES Cipher Block Chaining (AES-CBC) mode is employed which computes Message Authentication Code (MAC) or Message Integrity Code (MIC). MAC or MIC is then appended with unencrypted data and send to receiver. The code which is computed for MAC or MIC is composed of payload and header.
- **Confidentiality, Authenticity and Integrity of Data**. This level of security can be achieved by AES using both Counter Mode (CTR) and Cipher Block Chaining Mode (CBC) as shown in Table 5.3.

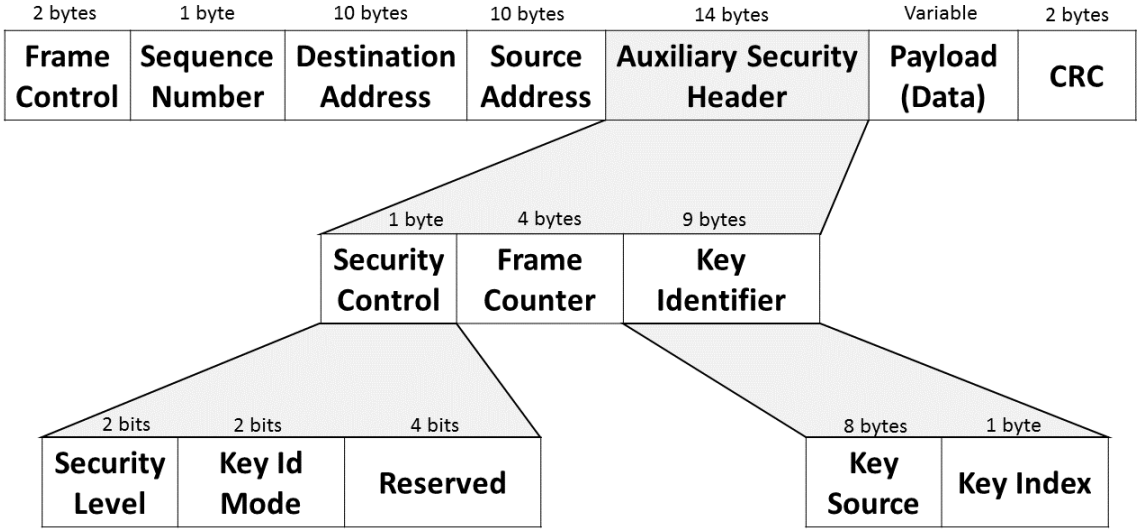

Figure – 5.1: Protected Data Frame in IEEE 802.15.4

5.3.3.2 Access Control Mechanism in IEEE 802.15.4

IEEE 802.15.4 also support access control mechanism allowing devices to use source and destination address for said purpose. The compliant devices store 255 entries pertaining to access control list (ACL).

5.3.4 Security Analysis of IEEE 802.15.4

Based on discussion carried out in this section, security analysis is proffered below with a view to highlight area to improve upon security: -

- Security is provisioned at MAC layer in IEEE 802.15.4.
- Security is optional, device may opt for security or no security.
- This standard does not define “Keying Model” based on classification of constrained devices i.e Class 0, 1 & 2 devices.
- Protection of data frames has been defined in the standard. However, no such mechanism has been specified for “Acknowledgement Frame” send by the receiver to originator.

5.4 6LoWPAN

Internet architecture is characterized by interconnected networks where IP packets crisscross between networks for desired operation and functionality. In IoT paradigm, IPv6 packets over IEEE 802.15.4 standard cannot be made to transmit /receive and impractical due to difference of MTU size specified in each protocol (MTU 1280 bytes vs MTU 128 bytes). In this context, 6LoWPAN provides the mechanisms for IPv6 packets

(MTU 1280 bytes) over IEEE 802.15.4 (MTU 128 bytes) enabled IoT devices; thus, an important technology to enable Internet connectivity in IoT architecture. 6LoWPAN creates compatibility among IPv6 and IEEE 802.15.4 by introducing header compression and packet fragmentation. 6LoWPAN based packets are prefixed by 6LoWPAN header, when transported over IEEE 802.15.4.

5.4.1 6LoWPAN Header

There are four types of headers specified by this standard, where first two bits of the header defines 6LoWPAN header. Following are the types of header: -

- **Non 6LoWPAN Packet**. Bits indicates that arrived packet is not meant for 6LoWPAN processing.
- **Dispatch Header**. This indicates that it supports compression of IPv6 header.
- **Mesh Addressing**. It implies the support for transmission of IEEE 802.15.4 packets, as needed to form multi hop network.
- **Fragmentation Header**. In this, fragmentation and reassembly of packets is supported to forward IPv6 packets over IEEE 802.15.4 enabled network.

5.4.2 6LoWPAN Compression

The dispatch header mentioned above provides information about compression mechanism applied to packet. Following are the methodologies for header compression:

- **LOWPAN_HC1.** This method does not support compression of global IPv6 address, therefore not suitable for IoT architecture.
- **LOWPAN_HC1g and LOWPAN_HC2**. These approaches provide compression mechanism for UDP headers and IPv6 addresses.
- **LOWPAN_IPHC**. This methodology provides compression mechanism both at link local addresses and local IPv6 headers.

5.4.3 Security Service in 6LoWPAN

6LoWPAN act as convergence technology for IPv6 and IEEE 802.15.4. It is highlighted that no security mechanism has been defined by 6LoWPAN. However, RFC 4919 has discussed employment of network security by using IPsec but impediment is very resource heavy operation of transport and tunnel mode of IPsec in resource constrained environment.

5.4.4 Security Proposal for 6LoWPAN

Keeping in view the absence of security mechanism in 6LoWPAN, following are the considerations for security researchers to offer security solution: -

- IPsec is an effective security solution at network layer. However, its applicability in IoT can be achieved by header compression and packet fragmentation. Gateway can be employed for translation among 6LoWPAN and IPsec.
- Rouge device in a network can forward duplicate or forged packets. This can occur because there is no authentication / integrity mechanism for packet in 6LoWPAN. In this context, introduction of nonce, timestamp and hash can bring authentication and integrity mechanism.

5.5 RPL

Routing over Low Power and Lossy Network (ROLL) group of International Engineering Task Force specified routing in 6LoWPAN network called as “Routing Protocol for Low Power and Lossy Network”. RPL is specified to support routing needs for simple and complex traffic models like multipoint to point, point to point and point to multipoint. In this regard, Destination Oriented Directed Acyclic Graph (DODAG) is the core element of RPL where each node in DODAG is aware of its own position and location of other nodes involved in routing of packets. Four type of control messages are used in RPL to maintain routing topology and to keep routing information updated. First, DODDAG Information Object (DIO) is used to maintain information pertaining current level of node, determine the distance of each node to route and selection of preferred path. Second message is Destination Advertisement Object (DAO) for upward and downward traffic by giving its destination information. Third, DODAG Information Solicitation (DIS) which is used by the device to get DIO message. Fourth message is DAO Acknowledgement (DAO-ACK) which is transmitted in response to DAO message. DODAG starts when the root node sends its position utilizing DIO message to all low power lossy network (LLN) levels. At every level, receiving routers notes parent path and participation path for all the nodes. Similarly, they send their own DIO message and consequently DODAG is constructed for entire network.

5.5.1 Security in RPL

RPL specifies security for routing control message by using security field after 4 byte ICMPv6 message header. In RPL code, high order bit defines whether the security is applied or not. The secure format of RPL control message is shown in figure 5.2.

Furthermore, security field also defines the use of cryptographic algorithm for security of packet.

1 Byte Type	1 Byte Code	2 Byte Checksum
Security		
Base		
Option(s)		

Figure – 5.2: Format of Secure Control Message

5.5.1.1 Security Modes in RPL

RPL defines three security modes which are as under: -

- **Authentication Mode**. Devices which intend to function as router in a network can employ this security mode. Initial association of the device to a network may involve utilization of preconfigured key and later on receives security key from keying authority to start operating as router. Authenticating the device is achieved by keying authority.
- **Preconfigured Mode**. In this security mode, devices utilize preinstalled symmetric key to associate with RPL network. The associated device can either act as a router or host in a network. Preinstalled key is used for authentication, confidentiality and integrity of control message.
- **No Security Mode**. As the name implies, RPL operate without any security.

5.5.2 Confidentiality, Integrity and Authentication in RPL

RPL specifies use of AES in Cipher Block Chaining Mode (AES-CBC) with 128 bit key and also RSA with SHA-256 algorithm for confidentiality, integrity and authentication. In this context IPv6 header, ICMPv6 and RPL message are not encrypted as these are required for decryption process. It is highlighted that RPL mandates use of asymmetric cryptography for authentication mode.

5.5.3 Security Analysis of RPL

Following points pertaining to security analysis is as under: -

- RPL standard restrict to the use of asymmetric encryption for authentication mode. However, it does not specify how to employ asymmetric algorithm for devices to function as router.

- RPL defines key management only in devices which are using preinstalled mode. It does not specify, key establishment in asymmetric cryptography for authentication mode.
- IoT network consist of different categories of resource constrained devices. In this regard, RPL do not specify employment of cryptographic algorithm and establishment of key agreement in such constrained devices.
- RPL does not define protection against internal attack; as an attacker with a node and keys can inject malicious routing message or to impersonate a gateway or to purposely drop legitimate packets.

5.6 CoAP

CoAP is designed by Constrained RESTful Environments (CoRE) working group of IETF. CoAP is as application layer protocol which employs metadata compression of application layer protocol without compromising interoperability. CoAP implement UDP over 6LoWPAN for communication among devices. CoAP is based on request and response model and uses Uniform Resource Indicator (URI) addressing for identification of constrained devices. This protocol allows communication between IoT constrained devices and other entities on Internet by employing CoAP or gateway for translating HTTP to CoAP and vice versa.

5.6.1 Messaging in CoAP

Messages are exchanged over unreliable UDP transport layer where CoAP offers reliability to transmitted messages by marking them as “Confirmable” and “Non-Confirmable”.

- **Confirmable Messages**. In this case, the receiver send acknowledgment to confirmable message. If the message is not received properly or error occurs, then receiver send Reset message.
- **Non-Confirmable Message**. In this scenario, receiving entity do not respond with acknowledge message.

5.6.2 Options for CoAP

In CoAP, information is exchanged by utilizing option(s) which includes critical, elective, safe or unsafe.

- **Critical Option**. In this, devices should understand and acknowledge each other.

- **Elective Option**. If the exchanged information is given an elective option, then devices may or may not respond with acknowledgment.
- **Safe Option**. Proxy has to forward the safe option even if not able to process it.
- **Unsafe Option**. Proxy has to understand unsafe option and process it before forwarding it.

5.6.3 CoAP Message Header

CoAP message format contains version field and 'T' field both having 2 bit each. Then, Token Length field (TKL) of 4 bits followed by Code field of 8 bits and Message ID of two bytes (16 bits). The Token field allows matching of request and response whereas Message ID provides reliability and detects duplication. The format of CoAP message header is shown in figure 5.3.

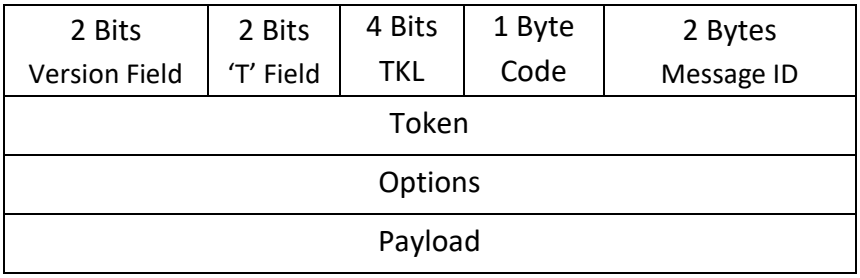

Figure – 5.3: Format of CoAP Header

5.6.4 Security Service in CoAP

Datagram Transport Layer Security (DTLS) provides protection to CoAP messages which implies that security to application layer is provisioned at transport layer, the way HTTP turns to HTTPs when TLS is employed. DTLS offers protection in terms of confidentiality, integrity, authentication and non-repudiation at application layer using CoAP. DTLS employs AES to meet security requirement for CoAP.

5.6.4.1 Security Modes

There are four security modes for the security of CoAP message.

- **No Security Mode**. As the name implies, no security is implemented for CoAP.
- **Pre-Shared Key Mode**. In this mode, security keys are preinstalled in constrained devices. This mode is suitable for those devices which does not support public key infrastructure. This mode mandates implementation of "TLS_PSK_WITH_AES_128_CCM_8", this means pre-

shared key of 128 bits on transport layer security is used by employing AES Cipher Counter mode and authentication achieved through pre-shared key and 64 bits nonce along with 64 bits integrity value.

- **Raw Public Key Mode**. In this mode, asymmetric keys are preconfigured in the devices which can be verified using Out of Band (OOB) channel. This mode does not employ certificates for private and public key. This mode is suitable for those devices which cannot take part in public key infrastructure. Elliptic Curve Cryptography (ECC) is implemented where devices authentication is carried out using Elliptic Curve Digital Signature Algorithm (ECDSA) and key agreement is done by Elliptic Curve Diffie Helman Algorithm with Ephemeral Keys (ECDHE). This mode mandates implementation of "TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8" security mechanism. This security mode also utilizes SHA-256 for computation of hashes.
- **Certificates**. In this mode, X.509 certificate is involved where devices can validate certificate. Thus, this mode is suitable for those devices which have sufficient computational resources to take part in certificate based public key infrastructure. Like Raw Public Key mode, key agreement is carried out by using ECDHE and authentication is done by ECDSA. This security mode supports "TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8" security mechanism.

5.6.5 Security Analysis of DTLS

Based on above discussion, security analysis of DTLS is as under: -

- Although DTLS is designed for resources constrained devices where different modes are offered for protection over CoAP but still initial DTLS handshake is computationally expensive.
- As CoAP uses UDP which involves fragmentation of packets; therefore, DTLS mechanism / process in the presence of fragmented packets raises requirement of processing power. Moreover, fragmentation may also require retransmission and reordering of packets; therefore, may result in added complexity in the presence of DTLS protocol.
- Gateway is required when DTLS is enabled when IoT devices needs to connect with Internet. Gateway will perform mapping between HTTP to CoAP and vice versa.

CHAPTER 6
IoT STANDARDIZATION AND IMPACT ANALYSIS

There are various standard bodies and consortium which are contributing towards IoT standardization; major standard bodies have been discussed in this chapter. Moreover, benefits of standardization are explained. IoT is evolving, there are various challenges to IoT standardization which have been described in this chapter. Impact analysis of present IoT standardization has also been carried out in this chapter. Finally, recommendations have been proffered for unified agreed upon IoT standard necessary for IoT success.

6.1 Introduction

Popularity of smart devices has amplified considerably over the last two decades [57]. Internet of Things (IoT) brings Internet connectivity for smart devices to develop human life comfortable, productive and safer [58]. For that reason, standardization is an important factor for the success of IoT [59], [60]. Initially, IoT enabling technology specified by various manufactures and research community were vendor and industry specific due to which they lacked end to end connectivity across different platforms. However, various bodies and consortiums are contributing towards consistency, compatibility and quality of protocols for IoT architecture. In IoT paradigm, a crucial factor to understand is that IoT needs variety of technologies to work collectively such as protocols at different layers, communication technologies, security and methodologies to interconnect devices across Internet arena. In this perspective, there are many standard bodies, consortium, organization, agencies and industrial groups as shown in figure 6.1 are functioning to formulate technical, legal and implementation standards but still a long way to achieve unified IoT standard; the way happened in the case of WiFi, TCP, HTTP and many other traditional protocols [61].

There is a wide range of standards available for IoT and it is difficult to cover each of them, so a handful of them are briefly discussed here with a view to identify challenges in standardization, to analyze impact of available standards and recommendations for unified IoT standard.

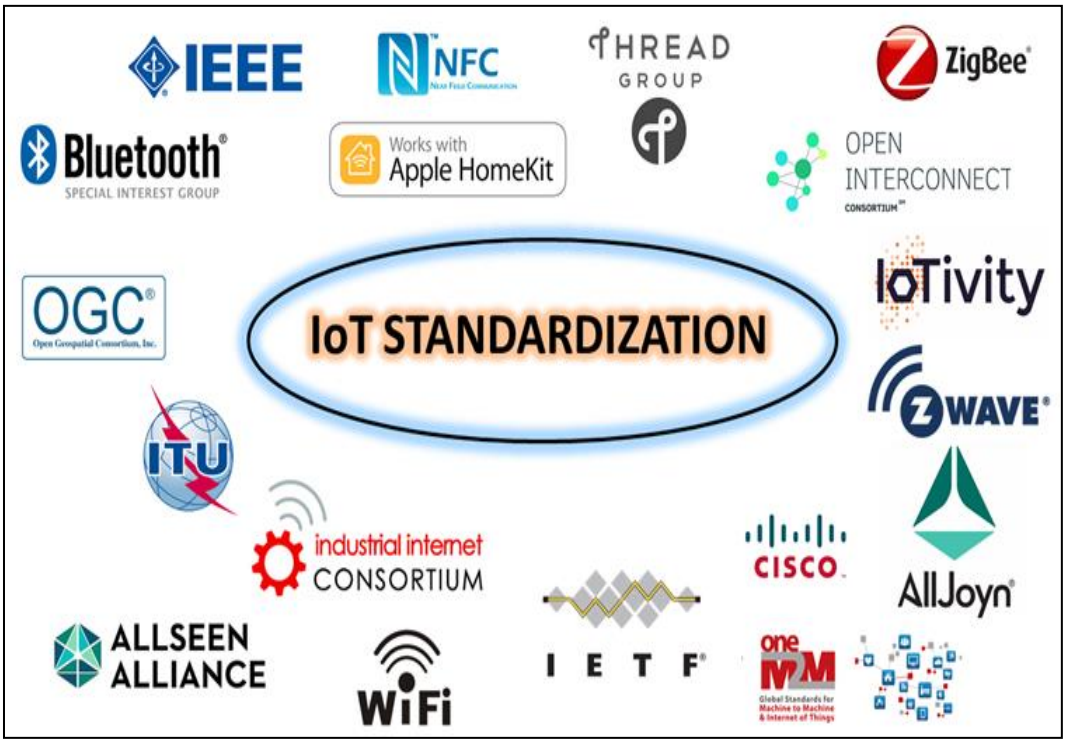

Figure – 6.1: IoT Standardization Bodies

6.2 Standardization and its Benefits

Process of standardization involves cooperation among developers, manufacturers, scientific community, firms, governments and users to create consensus for implementation of technical specifications [62]. In this context, following are the benefits which can be drawn from accepted and unified IoT standardization: -

- **Uniform Technology**. Establishment of uniform technology to implement globally.
- **Customization**. Minimal requirement of customization for deployment of IoT solutions.
- **Gateway**. Create an environment where entities can interact and collaborate without employing translation gateway.
- **Compatibility**. Achieving compatibility and interoperability of smart devices in a network.
- **Success**. On global basis, single standard can be an enabling factor for the success of IoT and prerequisite for broad adoption of smart interconnected devices.

6.3 Challenges to IoT Standardization

Many organizations, governments, standard bodies and consortiums are putting extensive work for standardization in IoT domain. Standardization plays a very important role towards technological consistency and conformity to regulations. As IoT is characterized by its heterogenous nature which introduces complexities in its architecture for which standards provides common platform for consistent functionality [63]. At the same time, IoT standardization is challenging due to issues in terms of technology, connectivity, diversity of devices and so on. Following are the areas which creates challenges for IoT standardization: -

- **Rapid Advancement**. Technological advancements in IoT is growing and evolving at a very fast pace which creates issues for standardization to keep up with rapid evolution.
- **Network Deployment**. Different network approaches for IoT deployment such as centralized, distributed and hybrid approach creates issues to come up with single standard for IoT architecture.
- **Classes of Smart Devices**. There are different categories of smart devices which are classified based on available resources in terms of processing, power, memory and bandwidth. Table 6.1 [36] shows classes of constrained devices in terms of RAM and ROM size. Hence, incorporation of such devices together with varying protocols and technologies in IoT architecture creates challenges for standardization process.

Table – 6.1: Classes of Constrained Devices

Device Category	RAM Size in Kbytes	ROM Size in Kbytes
Class 0	Less than 10	Less than 100
Class 1	10	100
Class 2	50	250

- **Communication Technologies**. Various communication technologies are available such as ZigBee, WiFi, Bluetooth Low Energy (BLE), Z-wave etc to enable connectivity among IoT devices [64], [65]. Each of these communication methodologies have its own strengths and weaknesses therefore needs careful deliberation to implement IoT solutions and offer standardized architecture.
- **Regional Regulations**. Different countries have their own respective laws and regulations pertaining to cyber licensing and crime. Standard bodies

offering regulatory documents needs to adjust and adapt to specific laws which is difficult to achieve.

- **IoT Range**. IoT devices needs to communicate beyond local network such as cloud infrastructure or devices over the Internet [66]. This wide range and flexible connectivity involves varying protocols, frameworks and technologies for which corresponding standard needs to be dynamic encompassing all players.
- **Fragmented Market**. Market is fragmented without a leader; everyone has its own IoT solutions and products by employing preferred protocols and technologies. Theoretically, even a small enterprise or entrepreneur is capable to offer IoT product. In such environment, it is very much challenging to formulate agreed upon unified standard.
- **Security Requirement**. Privacy and security concern based on consumer experience varies so much which adds hurdles in consensus for single standard.

6.4 IoT Standard Bodies

In IoT paradigm, aim of standardization is to achieve consistency, interoperability of product / services, quality, security, safety and unified approach for IoT implementation. In this context, the work on IoT standardization is in progress and still growing. There are many IoT standards and difficult to cover each of them here, so brief of major IoT standards as shown in figure 6.2 are as under: -

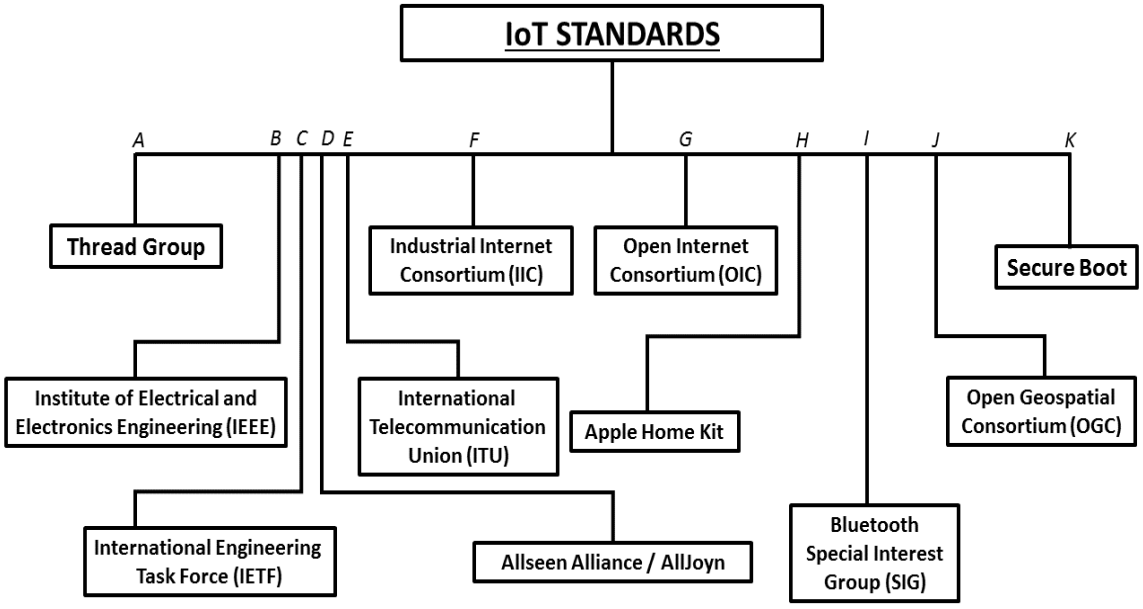

Figure – 6.2: IoT Standards

6.4.1 Thread Group

It is youngest among standard groups which covers protocols pertaining to networking with security, conservation of power and product compatibility. Thread group is a collaborative effort among Google's Nest and other companies including Silicon Labs, Samsung Electronics, ARM Holding, Philips, Qualcomm and others [67].

6.4.2 Institute of Electrical and Electronics Engineering (IEEE)

IEEE have number of standards which are directly related to create IoT ecosystem. More than 350 standards have been defined by IEEE which are applicable to IoT. The aim is to build architectural framework with the ability to support diverse IoT smart devices. In this regard, IEEE 802.15.4 is one of its early specification for low power radio operating in Industrial, Scientific and Medical (ISM) band [68].

6.4.3 International Engineering Task Force (IETF)

IETF work focuses on IP based protocols and connectivity among resource constrained smart devices. In this perspective, different IETF working groups have specified IPv6 Low Power Wireless Personal Area Network (6LoWPAN) and Routing over Lowe Power and Lossy Network (ROLL) protocols for IPv6 connectivity and routing of fragmented packets. Likewise, IETF Constrained RESTful Environment (Core) group specified Constrained Application Protocol (CoAP) for constrained devices at application layer [69], [70].

6.4.4 Allseen Alliance / AllJoyn

Initially, AllJoyn protocol was developed by Qualcomm in 2011 then shared the code with Linux Foundation in 2013. Both, Qualcomm and Linux Foundation created alliance called "Allseen Alliance" and enrolled members such as Microsoft, LG, HTC, Cisco and many others. Allseen Alliance offered framework which targets service layer functionality and connectivity for IoT devices. The aim is to create interoperability among devices which connect with other devices regardless of OS, platform or type of device [71], [72].

6.4.5 International Telecommunication Union (ITU)

ITU is contributing towards IoT standardization since 2005. It has formed a Joint Coordination Activity with a goal to share information with others in the field of IoT. In this context, SG20 standard has been specified for IoT technologies including M2M connectivity and ubiquitous sensor networks [73], [74].

6.4.6 Industrial Internet Consortium (IIC)

IIC was founded in 2014 and working towards industrial applications related to IoT. It is backed by various enterprises such as Cisco, AT&T, Intel and GE. IIC released its document covering characteristics of industrial internet architecture, security, privacy, interoperability and connectivity [75], [76].

6.4.7 Open Internet Consortium / IOTivity (OIC)

OIC has released a framework called “IOTivity” which covers device to device communications. Members of OIC includes Dell, Broadcom, Samsung, Wind River and others. OIC is in its early stages and expected to grow the passage of time [77], [78], [79].

6.4.8 Apple Home Kit

Home Kit is owned by Apple designed for communication and controlling of home appliances. It can be termed as proprietary way of offering smart solution to its consumer [80].

6.4.9 Bluetooth Special Interest Group (SIG)

It has announced Bluetooth Low Energy (BLE) device with the aim to exchange data among devices over short distances using short wave length to minimize power consumption. BLE utilizes short range radio with minimum amount of power to function for longer duration compared to earlier versions [81], [82], [83].

6.4.10 Open Geospatial Consortium (OGC)

Correct handling of location information in IoT has been addressed by OGC standard. There are 481 participants in OGC including different companies, governments, and universities contributing to develop IoT standard [84].

6.4.11 Focus Group on M2M (FG M2M)

FG M2M was established in 2012 with the objective to study M2M service layer requirements. Its main focus is “e-health” applications [85].

6.5 Impact Analysis of IoT Standardization

To reap benefits of IoT and to achieve its full potential, a unified accepted single standard is mandatory. Various foundations, organizations, consortium, standard bodies, industries and government are working towards ever growing IoT landscape. In the presence of these huge number of standardization bodies and offered framework, impact analysis of IoT standardization is as under: -

- **Competing Standards**. In global arena, many standardizing bodies are competing to offer their IoT standards. By no means, in the presence of these large number of standards IoT devices will be able to interact and collaborate universally.
- **Enterprise Support**. Heavy weight enterprises such as Samsung, Philips, LG, Intel, Qualcomm and many others are backing standard bodies of their own choosing. Therefore, lot many debates exist among competing parties to settle with truce and agreed upon IoT architecture.
- **State of Flux**. In recent years, many standard bodies have stepped in IoT domain and multiplying. Standardization of IoT is in a state of flux, no one is sure which one will make a difference or who all merge together to convey consensus and consistency in IoT standards.
- **Contesting Bodies**. Standard bodies such as Allseen Alliance and Open Internet Consortium agrees that there must be single accepted standard but irony is that both are fixed to their own standards. Thus, creates a predicament among competing bodies for single agreed upon IoT standard.
- **Selection of Standard**. In IoT, there are various technological layers for which there are many competing standards and some stacks have only few. This creates a dilemma for market players to select and adopt from many available protocols for IoT product or related services. Lack of uniformity creates complexity for product development; for example, one vendor offer smart e-health product and the other offer solutions for smart home but product connectivity and interaction from both the vendor is minimal due to lack of consensus on standard.
- **IoT Services**. In the absence of unified and single global IoT standard, vendors are not sitting idle and waiting for standards. Instead, offering IoT solutions and services in the market. This will introduce varying IoT products in the market which can create incompatible environment for future consumers using products from other vendors, thus will have negative impact on IoT success.

6.6 Proposal for Unified IoT Standardization

As mentioned above, prerequisite for IoT success and its global adoption is agreed upon unified standardization. Based on above discussion, following are the

recommendation to create positive competition and achieve consensus among standard bodies: -

- **Governments**. Cyber laws and regulations varies from country to country. At government level, collaboration among agencies and organization can create a platform to bring harmony on IoT standards in line with regulations of that specific region.
- **Pre-Standardization Groups**. Gaps among IoT research and development sector can be bridged by creating pre-standardization groups. After necessary deliberation, approved and refined recommendations on protocols / technology without inconsistency can be proffered to regular standard groups which will naturally create coherence among offered standards.
- **Working Groups**. At industrial level, working groups can be formed to formalize recommendations for standardization activities. In this context, regular workshops can be arranged to discuss enabling protocols and technologies to remove inconsistencies among industrial giants.
- **Parent Standard Body**. At global level, different standard bodies can be drawn under one umbrella by creating parent standard body for all. Although it is an ambitious approach and difficult but still plausible. Idea is to bring industry and standard bodies on one platform to present their document, based on agreed upon selection criteria a unified standard can be proffered for IoT architecture.

CHAPTER 7
SECURITY ANALYSIS OF IoT PRODUCTS AND LESSON LEARNED

Many IoT gadgets, product and services are available in today's market. In this chapter, few of IoT products have been explained and examined from security viewpoint. The products and their related protocol which are covered in this chapter are Fitbit Activity Monitors, Philips Hue Smart Lightening and Baby monitors and HomeEasy protocol. Finally, important lesson learned pertaining to security has been explained in this chapter.

7.1 Introduction

A "Thing" in IoT is a device which is having CPU, memory, software and network interface for communication. IoT tends to differ from traditional computing system due to absence of typical mouse, keyboard and other interfaces. Moreover, it is the "purpose" which differentiates IoT from traditional computers, IoT are single purpose objects rather than general purpose computers. As per Business Insider tech report published in August 2016, it is projected that by 2020, at around 34 billion devices will be connected to the internet [8]. The success factors for this adoption are low cost, simpler to install and automation it provides to the environment where installed. Compared to regular computing, IoT are constrained in terms of processing, memory, power and bandwidth capacity. Hence, implementation of traditional security mechanism in IoT domain is challenging and difficult to achieve. Likewise, majority of smart interconnected devices are short of upgrade and update mechanism once the product leaves manufacturer's production line. Moreover, smart devices are appearing over the Internet at an unprecedented rate which also include many "orphaned" devices which are unpatched and not updated. IoT has wide application range in different field of life such as military, agriculture, health, transportation and others. In this regard, IoT products / services which are available in the market are Fitbit, Belkin WeMO Switch, Nest Thermostat, Ubi Smart Speaker, LiFx Bulbs, Philips Hue Smart Lightening, Home Automation and many others. It is worth mentioning that due to low cost, autonomous operation, application in various sectors and constrained resources of IoT; these devices serve as bridgehead for malicious

actors not only to attack IoT devices itself but other connected devices over the web of Internet. Coupled with this, employees are also blurring the line between office and home network by working from home which is normally not secured as their office network; thus, allowing the attackers to exploit unsegmented network and IoT vulnerabilities installed at home to use as pivot for attack against IoT devices and traditional computing systems.

In this chapter, security weakness and privacy concerns of Fitbit Activity Monitors, Philips Hue Smart Lightening and Baby monitors along with Home Easy protocol as enlisted in Table 7.1 have been discussed with a view to draw lessons for improvement of IoT Security [86], [87], [88], [89].

Table – 7.1: Security Weaknesses in IoT Products / Protocols

IoT Product	Security Issues / Concerns	Exploit / Concern
Philips Hue Smart Lightening System	Global Master key for every device.	If master key is compromised, then security of all the devices is compromised.
Fitbit Activity Monitors	Device ID do not change and during pairing process ID of other devices in range is recoded and send to server,	Privacy concern and user can be tracked through static unique ID.
Gynoii Baby Monitor	Hardcoded Credentials.	Once credentials are exposed then device is open for remote access.
TRENDneT Baby Monitor		
Home Easy Protocol	Source ID is used for authentication purpose and sent unencrypted.	Attacker can intercept and access the devices.

7.2 Philips Hue Smart Lightening System

Consumer interest towards smart lights has considerably increased since 2012. Among various smart lightening solutions such as Osram Lightify, GE Link, LiFX and others; Philips is one of the most popular smart lightening system intended for residential purpose and can also be employed in hotels, offices, restaurant, hospitals and industrial buildings. Philips Hue Lightening System as shown in figure 7.1 consist of white colour lights, RGB colour lights and LED strips. These smart lights can be controlled through Android and iOS applications.

Figure – 7.1: Philips Hue Smart Lights

7.2.1 Philips Hue Architecture

General architecture of Philips Hue Smart Lightening System is as shown in figure 7.2. The lightening system comprises of at least one smart light which is connected to gateway or hub. The gateway is connected to Internet through home router via Ethernet of WiFi. In order to control the lights such as turning ON or OFF, changing brightness or color and to have remote access; application on mobile device is required to be installed. Consumer sends the requisite command through their installed application via Internet or home router to gateway which translates the received query for desired functionality. In addition, dimmer switches are also available to control the lights.

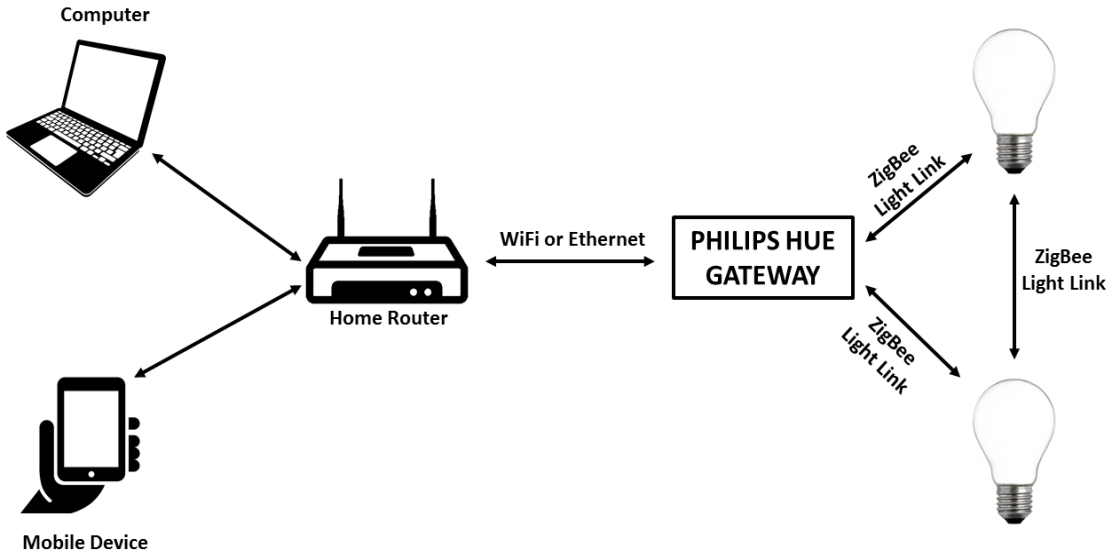

Figure – 7.2: Philips Hue Architecture

7.2.2 Technical Detail of Philips Hue Smart Lightening System

Philips hue operates by using ZigBee Light Link (ZLL) protocol [90]. ZLL itself is based on IEEE 802.15.4 designed for low power and low data rate devices. IEEE 802.15.4 specifies Maximum Transmission Unit (MTU) size of 128 bytes with data rate of 250 Kbps using 2.4 GHz frequency in ISM band.

7.2.2.1 ZLL Standard

Main features of this standard are as under: -

- Provides two procedures for setting up of ZLL network i.e. Classical Commissioning and Touch Link Commissioning.
- **Classical Commissioning**. It is a mechanism in which ZLL network is established or new device is incorporated to existing network. Device which intends to associate with a network transmit “beacon request” packet on different channels. The gateway replies with “beacon response” packet, if open for new devices. After association, gateway sends network key which is encrypted by global ZLL link key.
- **Touch Link Commissioning**. The gateway scans the network for the device by sending “scan request” packet on different channels. The receiving device responds with “scan response” packet. After this, gateway asks for more information by sending “device information” packet to which receiving device responds with “device information response” containing requisite information. Moreover, the device scanning process may result responses from multiple devices, out of which user needs to select one device for that “identity request” packet is send; upon receiving the identity frame, the device performs preconfigured identification action such as flashing of bulb for few times. After receiving “device information response” frame, the gateway then builds “network join end device request” frame which contains encrypted network key and sends the frame to desired device. Upon receiving, the device responds with “network join end device response” frame indicating successful association. The encryption and decryption is carried out by ZLL master key programmed in every ZLL enabled device.
- ZLL consist of four layers i.e. Physical (PHY), Medium Access Control (MAC), network and application layer.

- **PHY layer**. It uses 2.4 GHz in ISM band divided into 16 channels.
- **MAC layer**. It deals with access to radio channel using CSMA/CA mechanism, sending beacon, acknowledgement and synchronization frames.
- **Network Layer**. It provides functionalities regarding network topology, routing and security services.
- **Application Layer**. It provides the interface to end user to interact with smart system.

7.2.2.2 Security in ZLL

Security features offered by ZLL is as under: -

- IEEE 802.15.4 supports encryption and authentication mechanism but ZLL devices does not implement security at this level.
- Security is only employed at network layer by using AES-CCM with 128-bit network key encrypted by global master key. Every ZLL enabled device is programmed with global master key which is used to encrypt network key for secure communication.
- At application layer, no security is provisioned for the devices.
- Device verification mandates certain level of received signal strength. In other words, during verification process the device only respond if received signal is strong indicating that requesting devices is in close proximity. In Philips Hue Smart Lightening System, verification process works at around 30 cm of communication range. Device verification process will not be initiated if received signal strength is below threshold value.

7.2.3 Security Analysis of Philips Hue Smart Lightening System

Based on above discussed ZLL protocol and its security features, security analysis of Philips Hue Lights are proffered below: -

- The ZLL master key is provided to every certified manufacturer and bounded with Non-Disclosure Agreement (NDA). This global master key is preconfigured in every device which is then used to encrypt and decrypt network key for secure communication. In case, ZLL master key revealed by insecure product or extracted by any mean; then the secret key will not remain secret any more.

- Device verification process mandates close proximity so as to receive certain level of signal strength. Adversary can bypass this check by using modified radio with higher output power to scan / sniff the network from longer communication range. In other words, network can be deceived from long distances using high output power.
- During commission phase, frames are exchanged between devices. As there is no procedure defined to authenticate received frames therefore attacker can inject his own crafted frame for malicious purpose or to scan the devices in a network by sending scan request and receiving scan response. For this attack, adversary does not require to have global master key.
- The purpose of "identify request" frame during association process is to identify required device in a network. The bulb identify itself by blinking for few seconds. Malicious actor can abuse this frame to annoy legitimate user.

7.3 Fitbit Activity Monitor

Fitbit is an American company which develops wearable products to track activity and measures data such as heart rate, number of steps walked, sleep quality, distance travelled and few other metrics. Fitbit also have its associated mobile application and website to perform synchronization where user activity is forwarded to Fitbit cloud service over the Internet. The monitored data does not persist on the smart phone, tablet or computer, it is required to be fetched from Fitbit cloud service during synchronization. The synchronization process between Fitbit device and smart phone / computer is carried out by using either Bluetooth 4.0 or Bluetooth Low Energy (BTLE). On the other hand, synchronization between smart phone / computer is occurred over the Internet with cloud service using encrypted session. Components involved in Fitbit it system is as shown in figure 7.3.

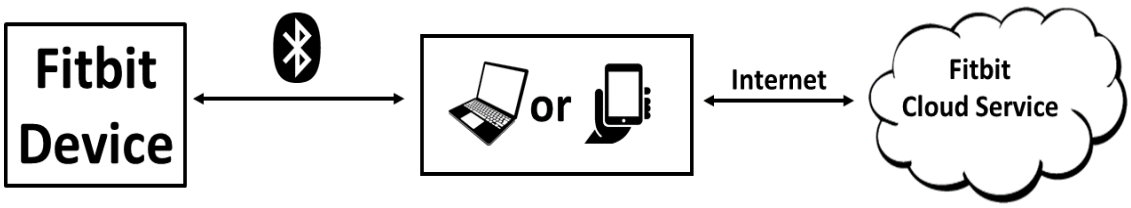

Figure – 7.3: Components in Fitbit System

7.3.1 Security in Fitbit

Salient of security features in Fitbit are: -

- Bluetooth 4.0 or BTLE is used for pairing among wearable device and smart phone / computer. Security inherent to Bluetooth specification is employed during pairing.
- Recorded data is encrypted and stored on Fitbit device using AES.
- Session between smart phone / computer and Fitbit cloud service is established over TLS connection.

7.3.2 Security Analysis of Fitbit

The synchronization / pairing process between Fitbit device and smartphone / computer is done using Bluetooth protocol therefore traffic in this medium can be actively sniffed. The captured traffic revealed following security concern pertaining to Fitbit: -

- Fitbit wearable device respond to broadcast send by the device in communication range. This allows to get the private Bluetooth address of Fitbit device. It is pertinent to mention that Fitbit device do not change their private address thus provides an opportunity to track desired user.
- During synchronization / pairing process, Fitbit application also give private ID to server of other Fitbit devices which are in range, if any. This shows that Fitbit can structure a profile around the user surroundings.

7.4 Baby Monitors

Baby monitors satisfies personal use requirements for parents. These monitors are sited near infants to observe and supervise their activity, get alerts when baby cries, listen and talk to comfort a toddler. These devices are accessed over the Internet helping parents to monitor when away from home and also allows distant family members to see their nieces, nephews and grandchildren. As these monitors are Internet connected devices therefore makes them an ideal target for malicious actor to annoy residents or to gain access to other devices in home network. Hence, making the compromised device to use as pivot to exploit other computing devices. Rapid7 has highlighted different vulnerabilities in their paper pertaining to baby monitors developed by different vendor and disclosed the same to concerned vendors, CERT and public. In this section, insecurities in baby monitors offered by two different vendors have been discussed.

7.4.1 Gynoii

Gynoii develops smart products aimed at helping infants to nurture in safer environments and making parent's daily life easier. Rapid7 disclosed vulnerability that Gynoii product is shipped with hardcoded credentials thus allowing access to anyone from local web. The detail of these credentials is as under: -

Username : guest or admin

Password : guest or 12345

7.4.2 TRENDnET

TRENDnET WiFi baby monitor allows the parents to monitor their baby over the Internet connection. After commissioning the device in a network, user can open a web browser or associated application to have live video stream on their smart phone, tablet or computer. Rapid7 has highlighted vulnerability in TRENDnET's WiFi Baby Cam TV_IP743SIC where credentials are preconfigured into the device. These devices can be accessed by anyone using Universal Asynchronous Receiver / Transmitter (UART) interface resulting into local and root level OS access. Hardcoded credentials are: -

Username : root

Password : admin

7.5 Smart Home

Smart home is equipped with smart devices and communication technologies which allows the residents to connect with installed devices and control their functionality according to their needs. In smart home, various components and appliances are interconnected to form a network where they communicate with each other and with inhabitants to perform requisite operation based on selected criteria. The primary goal of smart home is to bring comfort for inhabitants through autonomous operation and received instructions from owners. There are various vendors in the market offering home automation solution by employing different standards and protocols in their systems. Home Easy protocol is among one of many protocols which is used by vendors for home automation such as Byron, Proove, Anslut and others.

7.5.1 Overview of Home Easy Protocol

Home Easy enabled devices employ 433.92 MHz of frequency to exchange information [89]. The system uses amplitude shift keying technique to transmit and

receive codes. The device is connected to Internet using central entity which act as gateway or hub.

7.5.2 Security in Home Easy Protocol

This protocol operates by associating receiver to transmitter. In pairing process, a button on each receiving and transmitting device is pressed which allows exchange of ID from transmitter to receiver which is then compared with set of stored IDs. This ID is 24 bit and unique to each device, if the received ID matches with stored ID then pairing process becomes successful. This protocol also allows to transmit group command, each receiver in the group command act on received request provided that receiver has transmitter's ID stored with it. The packet format of this protocol is shown in figure 7.4. The complete frame consists of 32 bits where first 26 bit is the ID of transmitter which is unique and identifies the transmitter. The next bit indicates whether it is a group command or not. The next bit is about the state showing either the device needs to be switched ON or OFF. Next two bits is device code which indicates the receiver to be controlled. Last two bits is about the action which is to be performed such as up or down of window blinds.

Transmitter ID (26 Bits)	**Indication for Group Command** (1 Bit)	**Device State** (1 Bit)	**Code** (2 Bits)	**Action Value** (2 Bits)

Figure – 7.4: Home Easy Frame

7.5.3 Security Analysis of Home Easy Protocol

Based upon pairing process and functioning of group command, following are the security concerns pertaining to this protocol: -

- Security of devices is dependent on source ID and is not encrypted when transmitted.
- No encryption mechanism is employed in the protocol for security of transmitted information.
- An attacker after acquiring transmitter ID can impersonate for malicious activity.

- Malicious actor can cause DoS attack where attacker after impersonating can constantly send group command making impossible for legitimate transmitter to control receivers.
- Attacker can also change the bits in packet to ON or OFF the lights and control window blinds or door bell.

7.6 Lesson Learned

There are various building blocks of IoT, among many of them security is the one which is fundamental to its success. Security is not a onetime measure instead a continuous process which merits innovation and improvement to meet emerging challenges. In this section, only a few of IoT gadgets have been analyzed in order to draw some lesson for future IoT. Lesson drawn from some insecure design of IoT gadgets are as under: -

- Apparently, smart systems seem secure and robust as agreed upon specifications along with strong encryption is applied. But, in depth analysis and penetration testing reveals quite a few security holes. Therefore, before leaving the production line; the devices must be audited and thoroughly check for security vulnerabilities.
- Relying on global master key is not a suitable methodology for secrecy. In case of ZLL, master key pertaining to touch link commissioning has been compromised and exposed to world thus leaving security mechanism vulnerable to malicious actors. Even if master key is required for security of systems then it must be shared among devices through out of band (OOB) channel or changed after prescribed duration instead of hardcoding them into the devices.
- Access to IoT network and pairing process based only on received signal strength is not a viable option as an attacker can easily setup high output power by using software defined radio for malicious activity. Coupled with other security solution, the use of close proximity or signal strength is useful to increase security robustness compared to utilizing only received signal strength for security purpose.
- Effective security can be achieved if applied at all layers starting from physical to application layer. In case of ZLL, the security is applied only at network layer and not at MAC layer as offered by IEEE 802.15.4.

- Keeping static device ID may raise privacy concern for the users as it can provide an opportunity to track consumer using permanent device ID, as in case of Fitbit.
- Hardcoded username and password must be avoided. Mechanism to be in placed where user must change default username and password after setting up intelligent system.
- Authentication must be based on password or two factor authentications instead of mere exchange of ID between devices. In case, device ID is required to be used for authentication then it must be encrypted before exchange and changed after specified interval of time.

CHAPTER 8
CHALLENGES TO IoT AND IMPACT ANALYSIS

The goal of this chapter is to highlight major challenges pertaining to IoT. In this chapter, main constraints and majority of security concerns are explained. Based on discussed challenges, impact analysis has been carried out to highlight severity of discussed issues.

8.1 Introduction

IoT is a network of smart devices with the ability to detect and exchange information among themselves. IoT enables smart devices to connect physical world and virtual world. When smart device sense or detect its environment such as sensing the temperature; the device is creating a path to link physical world with virtual world. On the other hand, when a device is given instructions from Internet through an application interface to adjust temperature or open door lock then this operation connects virtual world with physical world. In IoT, physical objects become virtual thing having processor, memory, power and connectivity which allows to operate autonomously based on selected criteria or on received instructions. With these diverse functionalities and characteristics, IoT has potential to extend computing to “anything, anyone, any service” at “anywhere, anyhow, anytime” with a view to improve human life. In this perspective, IoT is an emerging domain of scientific, technical, social and economic community to further develop IoT technology and related aspect. At present, based on specified protocols and standards many IoT services are available in the market. Meanwhile, several challenges still remain for IoT vision in order to reap its potential benefits. Hence, IoT is a domain where research contribution is in full swing to address challenges for successful IoT architecture. One of the prime challenge that needs focus for success of IoT is its security. Without efficient and strong security mechanism, attacks against IoT will undermine any of its benefits.

8.2 Constrained Ecosystem

IoT devices are constrained in terms of processing, power, memory and bandwidth capacity. So, this creates unique challenges which are different from traditional computing system. The security solutions which can be employed in regular computing system cannot be used for security in IoT. In this context, IETF proposed classification of constrained devices which is based on RAM and ROM size [36]. The devices are categorized as Class 0, Class 1 and Class 2 devices as enlisted in Table 8.1.

Table – 8.1: Categories of Constrained Devices

Device Category	RAM Size in Kbytes	ROM Size in Kbytes
Class 0	Less than 10	Less than 100
Class 1	10	100
Class 2	50	250

8.2.1 Computational Ability

Compared to traditional computers, IoT objects are single purpose devices where they may be sensors, actuators or others. These devices need to transmit and receive the data or perform an action based on defined criteria in real time. Due to cost restrictions and specified functionality; processing capability is kept limited in these devices therefore implementation of security mechanism merits deliberation.

8.2.2 Energy Requirement

Power is the major concern of smart interconnected devices as they are battery powered and requires long operation time. Increasing computational power, data rate or communication range means more power consumption. Thus, selection of security solutions is critical with regards to power drainage as there is difference among different encryption mechanisms, key establishments, hashing algorithms and other software.

8.2.3 Memory

Memory in terms of volatile and nonvolatile (RAM and ROM) in IoT devices are limited. Flash memory is utilized for storage of data and application software whereas RAM is used as temporary memory for computational purposes. However, with technological advancement memory has been improved in term of size and capacity but still cannot meet the requirement of many algorithm and software in constrained device.

8.2.4 Bandwidth Capacity

To reduce energy consumption the radio needs to be energized for short duration, use high frequency and small payload for quick transmission. However, with higher frequencies the communication range reduces for which power output needs to be increased. Moreover, if encryption is used then it will consume processing, power and more bandwidth. Furthermore, increase in bandwidth means more processing and power consumption. Therefore, communication range, data rate and selection of frequency merits careful study of available resources i.e. computation and battery life.

8.3 Identity Management

Among many security challenges to IoT, identity management is one of the most important aspect in IoT protection. Identity management is the process which "enables the right individuals to access the right resources at the right time and for right reason" [91]. Identity management ensures the correct control of information about IoT entities where such information contribute towards authentication and authorization of an entity. Identity management is linked to security therefore enable the devices in a network to correctly access and collaborate among themselves and with other entities. In IoT ecosystem, huge number of smart objects and consumers creates immense challenge to implement and manage the identities of respective entities. It is not the technology or software which creates complexities in identity management but the heterogeneous environment where wide range of devices, protocol and software operates. Identity management involves consideration of following to create efficient mechanism for identification in IoT network: -

- A device identity cannot be the same as the identity of its prescribed functionality. The photocopier machine can have IP address but it must also have its own identity so as to distinguish itself from other photocopier machines in the network.
- IoT device can create its own identity through its specific features. A device installed for door lock mechanism can identify itself using its components and specified functionality.
- Devices must know the identity of their owner. In this case, the owner identify himself to the object and the object identify itself to the owner for intended purposes.

8.4 Authentication

IoT is characterized by its heterogenous nature where devices transmit or receive the data for prescribed functionality. Without authentication mechanism, there will be no way to ascertain that received data is from legitimate entity and the content it contains is not altered during transit. Identity management plays a vital role for authentication process as various entities needs to authenticate each other for trusted services. In this regard, related constraints such as processing, power, memory and bandwidth capacity needs to be considered and balanced to implement requisite authentication mechanism. Without proper authentication mechanism, it can create devastating impact on sensitive information. As mentioned earlier, IoT devices are resource constrained therefore today's strong authentication and encryption mechanism cannot be applied in such environment. Secondly, protocols pertaining to pairing, authentication and authorization involves some degree of human intervention in terms of configuration therefore IoT device accessibility is an important factor for initial configuration which requires protection from theft, tampering and other forms of compromises.

8.5 Authorization and Access Control

Authorization is a process of allowing requisite access to authenticated entity. In traditional computing system, sufficient processing, power and memory resources are available for authorization mechanism where entity provides credentials for defined functionality. However, in IoT it is important to consider available computational resources as constrained devices may have limited resources to implement authorization and access control mechanism. Moreover, in IoT domain both end user and device are distinct entities therefore merits distinct rights which creates complexities for access mechanism. Without proper authorization, adversary can introduce rouge device for malicious activity.

8.6 Availability

It is crucial that interconnected smart devices should remain available to its owner for intended functions. The device functionality can be effected due to malfunctions or malicious activity and may no longer remain available to legitimate user. Similarly, availability issues can be created due to battery drainage, theft or damage to device. In this context, security and requisite mechanisms at all layers starting from physical to application layer can address availability concerns. However, implementation of requisite solutions requires resources which are always limited in IoT ecosystem. Hence, careful study and planning is required to employ security solutions and administrative

mechanism according to available resources. Otherwise, an attacker can create issues pertaining to availability in following manner: -

- For energy preservation, IoT devices often enters into sleep state. In security perspective, it can create problems pertaining to firmware update and patching because after sleep state the device may not receive required update. In the meantime, if network is breached then malicious actor can also stop update process for nodes coming out of sleep mode.
- Without proper security, an attacker can limit the device functionality e.g. refrigerator may stop cooling or smart light starts behaving unexpectedly.
- Adversary can also change the device functionality e.g. climate control system designed to cool a room in summer but attacker has reversed the functionality from cooling to heating.

8.7 Multilayered Security

IoT network is a combination of various devices which may include sensors, gateways, mobile devices, cameras, RFID readers, and wearable devices rendering requisite services to end users. In this context, device security is of paramount importance to guard against tampering, theft, failing and malfunctioning. Inadequately secured IoT devices not only have their local impact but can also harm globally which the world has witnessed in the form of DDoS attack on “Krebs on Security” and domains name system (DNS) called “Dyn”. Adversary can have physical access or remote access to exploit IoT device vulnerability. Instead of destroying device in IoT network, an attacker can draw the sensitive information or can create IoT botnet. Similarly, an attacker can replace legitimate device with a rouge device for collection of data or to carry out any malicious activity. In such compromised IoT network, few of connected devices can be unplugged but few are difficult to disconnect such as smart utility meters, traffic control system or implanted health care device. Thus, security of IoT devices, gateway or controllers are critical issue and very challenging. Moreover, absolute physical security can be achieved however robustness of security can be increased by introducing multiple security feature at all layers.

8.8 Encryption and Key Management

Data encryption is classified into two categories, namely symmetric and asymmetric encryption. Both the encryption methodologies have their own advantages and disadvantages for computing systems. In IoT perspective where smart interconnected devices are involved for their prescribed functionality have limitation in terms of

computing power, memory space, energy availability and bandwidth capacity; therefore, asymmetric encryption algorithm complexity and its requirement for resources makes it difficult to implement in such environments. On the other hand, implementation of symmetric encryption is suitable for IoT ecosystem due to simple and small amount of calculations. However, both the encryption mechanism shares common problem in terms of key exchange and security of key. Moreover, in symmetric encryption the message authentication code is employed for authentication purpose but this increases packet size which causes considerable overhead on bandwidth, processing, power and memory requirement.

In encryption domain, key management involves key derivation, distribution, storage, refreshing and destruction after expiry. In IoT context, key agreement is the major challenge due to constrained resources which merits effective mechanism and employment of lightweight protocols.

8.9 Firmware Update

Patching and firmware update is important to fix potential vulnerabilities in computing devices after they leave production line. Firmware or software update and patching is crucial to security because any insecure implementation can create backdoors into devices. Wide range of IoT devices is designed to be employed for longer time frame compared to other traditional computing systems. In addition, these devices are employed in inaccessible environment which makes reconfiguration or update challenging and difficult. Furthermore, it is expected that these smart devices may live longer than many manufacturers and vendors who produced them thus leaving orphaned devices with no firmware and patching mechanism to plug security gaps. So, it can be anticipated that security employed during deployment may not be enough for complete lifespan as attack vectors are continuously evolving. Hence, vulnerabilities can persist for long duration and will put digital world exposed to exploitation. The long-term patch management and firmware update along with secure implementation poses considerable security challenges for developers and security professionals.

8.10 Privacy

Protection of privacy rights and its respect is fundamental factor for trust on interconnected smart devices and offered services. IoT comprises of huge number of smart devices designed to collect data about the environment in which they are installed and this collected data is frequently related to end user. The collected data is beneficial to consumer but at the same time also useful for manufacturer and service provider. Data

collected by IoT device and its utilization becomes a privacy concern when the end user who is observed have different privacy expectations pertaining to scope and use of that data. Normally, people are concerned about their privacy and want to know what all data is collected about them and their environment along with how this data will be used by other parties. In traditional computing systems, people are provided with notice, consent and terms of agreement to which the user agrees by click of a mouse button or pressing enter key on keyboard. Contrary to this, traditional privacy model breaks down in IoT ecosystem where users do not have any mechanism to interact. In IoT, users are frequently not provided with interface to setup their privacy preferences and in many cases, do not have awareness or control about the data which is being collected and utilized. This creates immense gap between consumer privacy setup and the way the data is collected by IoT devices. Hence, IoT poses a huge challenge towards privacy concern pertaining to owner of IoT system.

8.11 IoT Botnet

Security for IoT devices is of paramount importance to guard against tempering, theft and changed functionality. In near future, the world would see explosion of smart interconnected devices and with this huge adoption the attack surface for hackers will also increase. In fact, the probability of IoT devices to become attack vector is high due to variety of cheap devices manufactured with minimal protection. Practical manifestation of this the world has recently seen when thousands of compromised IoT devices were used as IoT botnet against “Dyn” and “Krebs on Security”. In this context, requisite authentication, authorization and access mechanisms are vital and must be enforced by considering available device resources.

8.12 Jamming of IoT Devices

As IoT devices have limited processing, memory, power and bandwidth capacity therefore jamming attack is far more effective against them. Since, smart interconnected devices communicate utilizing wireless technology therefore the prime methodology for attacker is to carry out jamming attack. Alternatively, wireless communication media can experience interference from other co-located devices thus can create unintentional jamming. In any case, device will not be able to communicate among each other thus a major challenge in IoT domain.

8.13 Embedded Security

Security by design methodology involves implementation of security software, secure storage, secure hardware and secure communication interface during

development process. IoT device are single purpose devices compared to traditional computing systems, therefore onboard computational, memory, power and bandwidth resources are kept according to prescribed functionality and not for security purposes. Secondly, it is the cost which drives hardware design and onboard resources. Furthermore, usually security is not always the first priority but an add on feature. Cost and limited resources always restrict to implement security as a design feature. Embedded security in IoT ecosystem is challenging and merits detailed considerations to create balance between security mechanism and intended functionality of a device. Moreover, a thorough tradeoff analysis is also required at an early design and development stages to make appropriate technology to combat against security challenges.

8.14 IoT Standardization

In IoT paradigm, goal of standardization is to bring consistency, interoperability, quality of service, security and unified approach for IoT deployment. There are various foundations, organization, standard bodies and industries which are contributing towards standardization of ever growing IoT technology. To reap benefits of IoT and its full potential, there is a need to have unified agreed upon standard. However, in global arena there are many standard bodies competing to offer their own IoT standard and are backed by different heavy weight enterprises. Moreover, in recent years many standard bodies have moved into IoT Standardization and multiplying; thus, putting IoT standardization in a state of flux and no one is sure which one will make a difference in IoT standardization. Meanwhile, IoT standardization is itself challenging due to growing technical advancement, different network approaches (centralized & distributed), different classes of devices, regional regulations, fragmented market and other factors.

8.15 Interoperability

In traditional computing system and Internet connectivity, backward compatibility and interoperability is the fundamental feature allowing different system to talk to each other; thus, created huge impact on it success and economic growth. For IoT, an interoperable environment provides the platform for smart interconnected devices to communicate with other devices or systems for desired functionality. Interoperability for IoT is vital with regards to both consumer and vendor; since, interoperability allows to select devices with best features at low cost and integrate them in their already installed IoT environment or deployed services. In case of inflexibility, IoT users will be hesitant and will not opt for such incompatible devices. In IoT domain, interoperability has substantial influence on its adoption, success and potential economic growth; as

compatibility and interoperability encourages innovation, new research, dynamic services and provides efficiency to reap full benefits. Compared to traditional computing systems, interoperability is more complex and challenging in IoT due to varying degree of communication methodologies, availability of different protocols at same stack, proprietary solutions, lack of unified agreed upon standard and different security requirements. In this regard, contribution from research communities and standardization bodies can play a fundamental role to bring interoperability in IoT.

8.16 Impact Analysis

Among many, few major IoT challenges have been discussed in this chapter to highlight their importance and potential impact in different areas. If challenges and threats are not addressed appropriately in IoT systems then it can create considerable implications for end user, service provider and IoT manufacturers. Compromised IoT network can cause human injury, leakage of sensitive data, economical loss, disruption in services and many others. In this section, only a few of implications pertaining to IoT threats are analyzed with a view to highlight the damages it can cause.

8.16.1 Human Safety

IoT devices are designed to perform autonomous operation, send requisite data to end user and function on predefined criteria so as to improve quality of life and bring ease for daily working routines. As IoT converges physical world and virtual world therefore any security gap can compromise human safety. In public sector, such as electrical distribution or transportation system; any malfunction or malicious activity can break down entire infrastructure. Similarly, malicious exploitation of smart devices in health sector especially used for patients to monitor heart rate, blood sugar level and other medical condition can seriously endanger human lives. It is therefore imperative that security must be given priority to IoT architecture.

8.16.2 Service Availability

IoT has it its application in almost all fields of life such as agriculture, transportation, military, health, industry, banking, electric distribution, automotive, water distribution and many others. Consumer are concerned with availability of services for which end user has subscribed or invested to install requisite system. However, any security loophole or fault in IoT system can cause system down time for its intended user which may create economical loss or safety hazard. For example, water distribution system controlled and monitored by employing IoT technology can suffer down time if

smart connected devices are compromised due to non-implementation of security solutions.

8.16.3 Attack Surface

As per Business Insider tech report published in August 2016, it is projected that by 2020, at around 34 billion devices will be connected to the internet. Similarly, according to Verizon report “State of the Market: Internet of Things 2016” published in April 2016 states that 9.7 billion devices were there in 2014 which is likely to increase more than 25.6 billion by 2019 and this figure will cross more than 30 billion in 2020 all around the world. With this exponential growth of smart interconnected devices, the attack surface for attacker will also increase. Availability of large number of connected devices can create options for attacker to exploit vulnerability in connected device and use as pivot to attack other connected devices. Practical manifestation of this the world has recently seen in terms of attack against domain name system “Dyn” in 21 October 2016 and blog “Krebs on Security” in 13 September 2016, where attackers exploited weak credentials in IoT devices to use them as IoT botnet.

8.16.4 Reputation

IoT has its wide application in many sectors and has potential to bring huge capital for service providers and manufacturers. As per Business Insider tech report it is estimated that in next five years nearly $6 trillion will be invested in IoT sector; likewise, according to Verizon report IoT spending will grow to an estimated $1.3 trillion by 2019. This shows, IoT has bright business prospects for manufacturers and services providers but mandates trust and confidence by their consumers. Any vulnerability in IoT architecture will create threat environment to be exploited by malicious entity. Any breach or service down time can dent the trust and damage the reputation resulting into huge economic loss.

CHAPTER 9

PROPOSED SOLUTIONS TO CHALLENGES IN INTERNET of THINGS (IoT)

The goal of this chapter is to propose security solutions to IoT. In this chapter, considerations for IoT developer and designer have been recommended to achieve embedded security (Section 9.2). Two lightweight key establishment framework have been proposed, one involving out of band (OOB) channel and other involving trusted third party (Section 9.3). Interconnectivity and provisioning of services pertaining to IoT services can primarily be achieved through centralized and distributed network deployment. IoT deployment model based on central approach has been suggested for IoT network to achieve security and interoperability of connected devices (Section 9.4). Finally, security guidelines have been enlisted to achieve security for IoT at different layers (Section 9.5).

9.1 Introduction

Internet of things (IoT) is characterized by its heterogenous nature and interconnectivity where smart devices interact with each other for data and wide variety of services for consumer. Focal attraction of IoT is its real-time operation to collect and send data for processing, automated notification and ability to perform prescribed operation autonomously. Based on these features IoT has its application and utility in every field of life and adopted in agriculture sector, healthcare, banking, automotive industry, military and so on. It is cost effectiveness, interoperability, seamless connectivity, scalability, autonomous operation and extensibility due to which notion of IoT has spread all around the world and has towering future prospects in terms of adoption. But this huge scale adoption is linked to security challenges where people and organizations are concerned about privacy and security. Large scale interconnection of smart device all around the world will also increase attack surface for adversaries compared to present day interconnected devices thus creating immense challenges to address security concerns. Traditional security solutions, methodologies, techniques and

procedure involves implementation of security mechanisms such as firewalls, IDS, IPS, edge routers, antivirus, HTTPS, IP Sec, VPN, RADIUS server, encryption algorithm, biometric, RFID, SSL/TLS and many others. In this context, the key question is “can these security solutions be employed in IoT architecture for security”. To answer, considerations pertaining to constrained resources in IoT smart devices such as processing capability, power availability, memory and bandwidth capacity must be examined and analyzed. Likewise, key elements such as wireless connectivity and device mobility introduces added security requirements for IoT ecosystem.

9.2 Design Considerations for Embedded Security

Security challenges can be effectively address, if security is introduced prior to development and deployment of IoT network. Add on security features or security after production not only reduce the effectiveness of information security but also not efficient in terms of effort and cost to employ. Embedded security provides protection by design, improve performance, offer reliability and reduce expenditure in establishing secure network. In this context, embedded security is an effective mean to manage different security issues which can be introduced at hardware level, kernel level, operating system level and application software level. When considering to design, and develop secure IoT system, there is a need to emphasize on major constraints associated with IoT devices; these are processing power, energy requirement, memory and bandwidth limitation. If there are no such constraints then probably such design and development is dealing with regular desktop computers, not with IoT. Moreover, a detail trade-off analysis is also required at an early design and development stage to make the right technology which can deal with security challenges. Introduction of embedded security merits assessment pertaining to processing, power, performance and time to market which can help to make sure that the end product is both inexpensive and secure. Security by design architecture is based on secure software, secure hardware and secure communications. Following are the recommended design consideration as shown in figure 9.1, if applied then device security can be an embedded feature instead of an add on feature: -

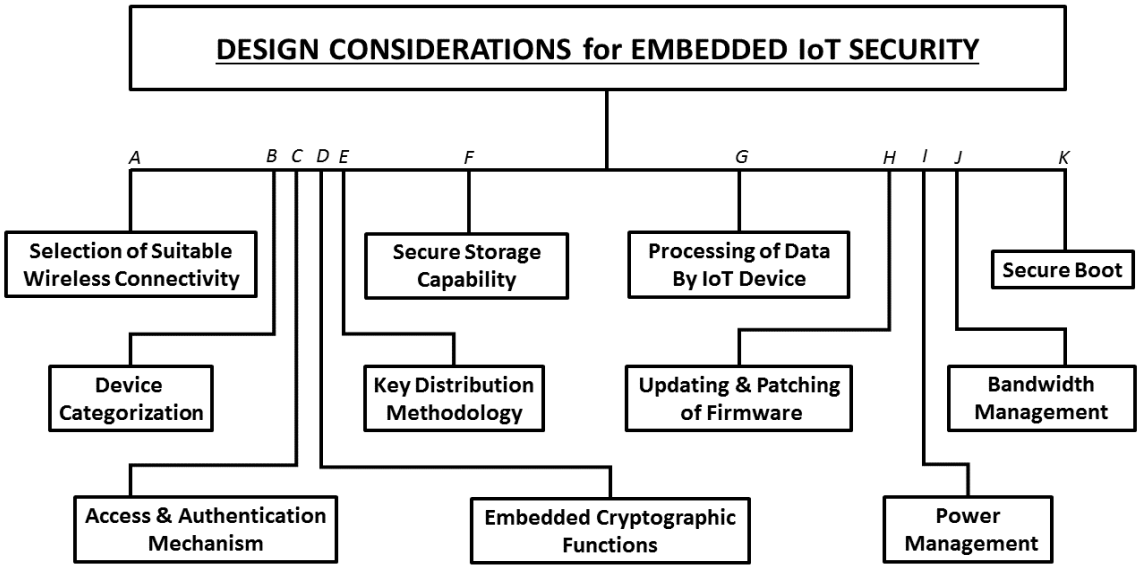

Figure – 9.1: Design Considerations for Embedded Security

9.2.1 Selection of Suitable Wireless Connectivity

The future of internet is IoT, where smart devices will be interconnected using different communication technologies to perform their prescribed task [24]. These smart devices will be connected to each other in a network utilizing a wide range of wireless technologies such as WiFi, Z-wave, Bluetooth, ZigBee etc. [25]. In this context, link budget, power consumption and cost are the major consideration for selection and employment of wireless technology. Many of the devices around us operates at 2.4 GHz, and many believes that 2.4 GHz will be the de facto choice to interconnect IoT devices. Transceivers based on 2.4 GHz has a short range, poor wall penetration and high power consumption. Moreover, this spectrum is crowded thus subjected to interference from various object using 2.4 GHz. On the other hand, transceivers based on sub GHz such as 900 MHz offer low data rates, provides long range communication and have less power consumption compared to 2.4 GHz radios. This spectrum is less crowded thus interference from other objects is also less. Designer must evaluate high and low frequencies of ISM band for particular environment where selected frequency is best suited to serve the purpose. In this context, designer and developer classify the devices according to their prescribed functionality, data rate requirement, power consumption, communication range, output power and interoperability. For example, smoke detectors, door sensors, climate sensor, tracking devices and others requires low data rate, long communication range and extended battery life. Thus, IoT devices can be classified based on their outdoor and indoor operation. Outdoor devices and indoor devices spread in large building can be

allotted sub GHz frequency as their numbers can be more compared to IoT devices installed in close vicinity. Conversely, indoor units (LAN) or PAN devices can be given high frequency of ISM band. For designers and developers, use of sub GHz frequency is one of the recommended consideration in IoT network. Sub GHz radio can save processing capability, power and leverage better management of network resources. In terms of security perspective, following are the advantages of using sub GHz frequency in IoT ecosystem: -

- Conserved power becomes available for built-in security mechanisms in IoT device.
- Less hop / repeaters will be involved, thus not only reduce or save the cost on repeaters but also prevent compromised repeaters to affect the security. For example, pollution attack can be prevented by not allowing repeaters to forward manipulated transmission.

9.2.2 Device Categorization

IoT network contains wide variety of devices and each device may be operating on different protocol. However, the functionality is same, that is to collect data or to perform an action. Achieving device security is reasonably challenging as IoT devices are constrained in terms of processing, power, memory and bandwidth. Small size and constrained environment of IoT creates complication to implement security at hardware level. Efficient design creates space for embedded security mechanism in IoT devices. Categorizing IoT devices according to their functionality and communication requirement can help designer and developer to efficiently manage hardware resources. Keeping in view the connectivity requirement and prescribed functionality, following are the design consideration to create resources in constrained devices for embedded security: -

- **Devices with Transmitting Module Only**. IoT devices interact with each other using a given communication technology such as WiFi, Bluetooth, Z-Wave etc. Devices with a functionality to only sense the surrounding can be design to transmit collected data. IoT devices such as sensors do not require to receive any transmission instead they are intended to sense and transmit the sensed information. Including only transmitting module and not incorporating the receiving mechanism will create space for embedded security mechanism in a device. Such IoT devices will not accept malicious instructions from attacker, thus protected from poisoning, hijacking, jamming and wide variety of attacks which requires a device to accept

instructions. As far as configuration, pairing or authentication is concerned; the requisite parameters be stored in the device to whom the data is to be transmitted.

- **Devices with Receiving Module Only**. IoT network have various devices which are intended to operate based on received instructions such as actuators. These devices can be designed with only receiving module to save power and silicon area for embedded security mechanism. Without transmitting capability, the compromised device cannot be made to act as botnet/zombie thus reducing the attack surface for an attacker. Requisite authentication parameters saved in such type of devices can allow only to receive instructions from legitimate or trusted entity.
- **Devices with Receiving and Transmitting Capability**. IoT network also have devices which needs to transmit and receive for prescribed functionality such as routers, gateways, CCTV cameras etc. This type of devices can be made secure by controlling their output power and use of symmetric encryption. Controlling output power avoids threats like interception and man in the middle attack whereas symmetric encryption provides confidentiality and authentication to transmitted data.

9.2.3 Access and Authentication Mechanism

IoT infrastructure creates challenges to support authentication and access mechanism where large number of smart objects attempts to connect a network or required to be accessed by an entity [25]. Addressing security challenges necessitates to understand characteristics of IoT devices and the technology that energize IoT infrastructure. Primarily IoT is characterized by constrained devices therefore implementation of access and authentication mechanism is challenging. These mechanisms must be optimized and light weight to meet the desired requirements. One of the vital design consideration is to keep minimum ports on a device and do not introduce network ports. NFC connectivity can be introduced to configure the device in a network for authentication or pairing. In this context, access and authentication mechanism must be made robust by combining authentication mechanism and introducing two factor authentication. Moreover, RFID can also be incorporated to authenticate devices in a network.

9.2.4 Embedded Cryptographic Functions

Security mechanism can be deliberated at an early stage when designing silicon chips and printed circuit boards. The dedicated integrated circuit for cryptographic function is the building block for confidentiality and integrity which depends upon type, functionality and category of the device [26]. Devices with light weight encryption at hardware level will create built-in security for secure authentication and to secure the data, thus addresses privacy concern in IoT architecture. Moreover, signature algorithm can be used to authenticate the data and avoiding injection attack. Furthermore, homomorphic encryption is another methodology where computation is carried out on cipher text without being decrypted. Although this technique is in its early stages, but in future can be introduced at hardware level to handle small data.

9.2.5 Key Distribution Methodology

Security issues like privacy, authentication and authorization are the major concern of end user in IoT architecture. In this regard, efficient key distribution mechanism is required for security of data and the device itself. Unencrypted exchange of keys over the network is not a viable option as it would compromise the system, as no one can say for sure that adversary has not intercepted the key. Keeping a predefined key at hardware level is also not a recommended solution because change of key will be nearly impossible, if compromised. So, there is a requirement to have secure key distribution mechanism among the entities. To address this following are the recommended options: -

- **Pairing Process**. To achieve secure key distribution or establishment mechanism, a simple push of a button along with manual input of code can server the purpose. The push of a button will secure the device from remote adversary whereas code input will protect the device if the attacker has physical access, thus preventing remote and local hijacking of smart object in a network.
- **Liquid Crystal Display**. Liquid Crystal Display (LCD) can be introduce to input the key or to use Quick Response (QR) code for secure pairing of device in IoT network.
- **Sound**. Voice can be used for secure pairing, where built in microphone on receiving device will pick up the sound which is then decoded into key. The decoded key can be displayed on LCD or played through the speaker.

- **NFC**. Near Field Communication (NFC) can be used for secure exchange of keys. NFC communication range is about 10 cm; so, unencrypted key distribution can be safely carried out as interception at such range is not possible.
- **Unique Keys**. At hardware level, finger print recognition, face recognition or voice recognition can be introduced to serve as unique key.

9.2.6 Secure Storage Capability within Device

In IoT network, there can be devices which do not require local storage of data and just send the notification to end user or to carry out predefined operation based on collected data. On the other hand, there can be devices which require data storage for necessary processing or devices may not have network access at all times therefore the stored data is sent as when the network connectivity is available. Moreover, there may be devices which do not necessitate continuous transmission of collected data, however, required to upload the data when needed thus needed to locally store the data. Similarly, storage capability may be needed for the programs which process the data, configuration of device, updating etc. In such cases, designers and developers have to make policy decisions about: -

- Amount of data to be stored on the device.
- Reserving the space for new code, update etc.
- How to secure the data, that is selection of light weight encryption algorithm.
- When to store the data.
- How long the data is to be stored, so that the data should not reveal the entire information if the device is lost or accessed by an adversary.

9.2.7 Processing of Data by IoT Device

With the technological advancement, the processing power of small devices are increasing day by day. But, processing is directly proportional to power consumption, more processing means more power drainage. Devices in IoT network which collects the data and individually asking backend device or server for processing of every new measurement, which in most of the cases is not an efficient methodology. Instead, such devices can process the collected data and perform the preset functionality. In processing, the device needs to have code and that code is to be stored on the device to process the collected data, therefore, device with processing capability also need storage

capability. Devices which carry out processing and storage must have strong encryption at hardware and application level to address confidentiality and integrity of data.

9.2.8 Updating and Patching of Firmware

Updating and patching is important to remove flaws or to improve functionality of IoT device. In early stages of design process, it is essential to consider that how to update and patch the firmware when the product is going to leave production line. The post production updating and patching potentially improve security of device but at the same time can open up the avenue for attacker to rewrite firmware remotely and compromise complete IoT network. Use of built in authentication and certificates can be utilized to update the firmware when delivered by manufacturer. Such built in feature can prevent the attacker to upload malicious code.

9.2.9 Power Management

Processing capability and networking is dependent upon availability of power. Power is the main differentiator for the functionality and operation of system. It would not be wrong, if one can say that security is dependent on power because it is the integrated circuits (ICs) which carries out processing of security algorithm. In IoT network there can be devices with unlimited power and at the same time devices with limited power, hence, power has a major contribution and merits efficient management. IoT devices with unlimited access to power are generally connected with home appliance such as refrigerator, air conditioning systems, audio video systems, cars, kitchen appliances etc which have constant power source and in turn also provide power to IoT devices associated with them. IoT device with limited energy source are smart watches, health sensors, trackers and other devices connected to limited power source such as batteries. Power management is of paramount importance for IoT devices to perform their functionality and security operations. In this regard, recommended consideration for power management are: -

- **Radio Operated Devices**. Radio (WiFi, Bluetooth etc) operated devices may be designed to transmit data when needed or required.
- **Data Size**. Transmitted data to be of small size, consequently energizing the transmitter module for a short duration and saving the power
- **BTLE**. Light weight communication protocol such as Bluetooth Low Energy (BTLE) can be utilized.
- **Output Power**. Low output power for wireless communication can aid in conserving the energy.

- **Power Saving**. Power saver technique can be utilized for radios to schedule wake up and sleep timings.
- **Processing Speed**. Use of high processing speed will help to complete the task in short time and entering into sleep mode fast can preserve the energy.

9.2.10 Bandwidth Management

Effective management of bandwidth can also help to put less constraint on power and processing requirement. Conserved processing capability can be utilized for security protocols and procedures in IoT device. In this context, following are factors which may be considered for efficient bandwidth management in IoT network: -

- **Light Weight Software**. Use of light weight encryption algorithm like REACTAANGLE, BLAKE etc
- **Optimized Protocols**. Use of optimized protocols such as CoAP, DTLS, 6LoWPAN, QUIC etc.
- **Packet Size**. Reduced packet size without compromising the security when transmitting or receiving can conserve processing and power for implementation of security mechanism.
- **Transceiver Use**. Transmitting and receiving the data as and when required, instead constant use of transceiver to conserve power and processing capability.

9.2.11 Secure Boot

When a device start, the secure boot functionality checks the signature of software so as to avoid loading of malicious programs. In other words, functionality of secure boot is to start the system to an accepted and reliable state. Maintaining secure boot feature in IoT device at design phase will secure the intended functionality of device

9.3 Proposed Lightweight Key Establishment Frameworks

IoT architecture is characterized by its heterogenous nature where majority devices are resource constrained in terms of computing, power, memory and bandwidth. This imbalance in resource capability among IoT devices creates challenges for provisioning of end to end security. Protocol which are employed for general purpose computing like Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP), Transport Layer Security (TLS), public key cryptography and others are very much resource heavy to be implemented in resource constrained IoT environment. In IoT network, security solutions need to be as reliable and secure as designed for traditional computing and at the same time puts less computational and communication overhead.

Encryption is classified into two categories, namely symmetric and asymmetric encryption. In IoT, key establishment among entities is challenging due to constrained environment. As far as encryption key is concerned, it falls under two categories that is stream cipher key and block cipher key. Block cipher employ secret key on block of data whereas stream cipher applies secret key on a data stream bit by bit. In this context, two frameworks for key establishment pertaining to block cipher have been proposed.

- Key establishment between two devices involving Out of Band (OOB) Channel.
- Key establishment between two devices involving trusted third party.

9.3.1 Proposed Light Weight Key Establishment Framework Involving OOB Channel

This framework is based on Pre-Shared Key mode (PSK) where symmetric key is established and agreed upon at both the IoT devices. A "Common Secret Value (SV)" is exchanged among entities using OOB channel. Based on SV, a Secret Key (SK) is derived and then refreshed after specified duration. Salient of this framework is as under: -

- Two entities involved in key establishment scheme i.e. Device A and Device B.
- Device A has MAC address (M_A) and unique identity (ID_A).
- Device B has MAC address (M_B) and unique identity (ID_B).
- Both the entities know each other MAC addresses and identities.
- Initially, resource constrained IoT devices 'A' and 'B' exchange Common Secret Value (SV) using OOB channel which is assumed that not controlled by adversary.
- Random number (RN) is generated for Secret Key (SK) derivation at both ends.
- RN is encrypted using lightweight encryption algorithm e.g. PRINCE, BLAKE, RECTANGLE etc. Selection of encryption algorithm (ENC) is at the discretion of IoT designer or manufacturer.
- After specified interval of time, Fresh SK is derived.

9.3.1.1 Step by Step Process of Key Establishment Framework

Workflow of proposed key establishment process is shown in figure 9.2 and explained below: -

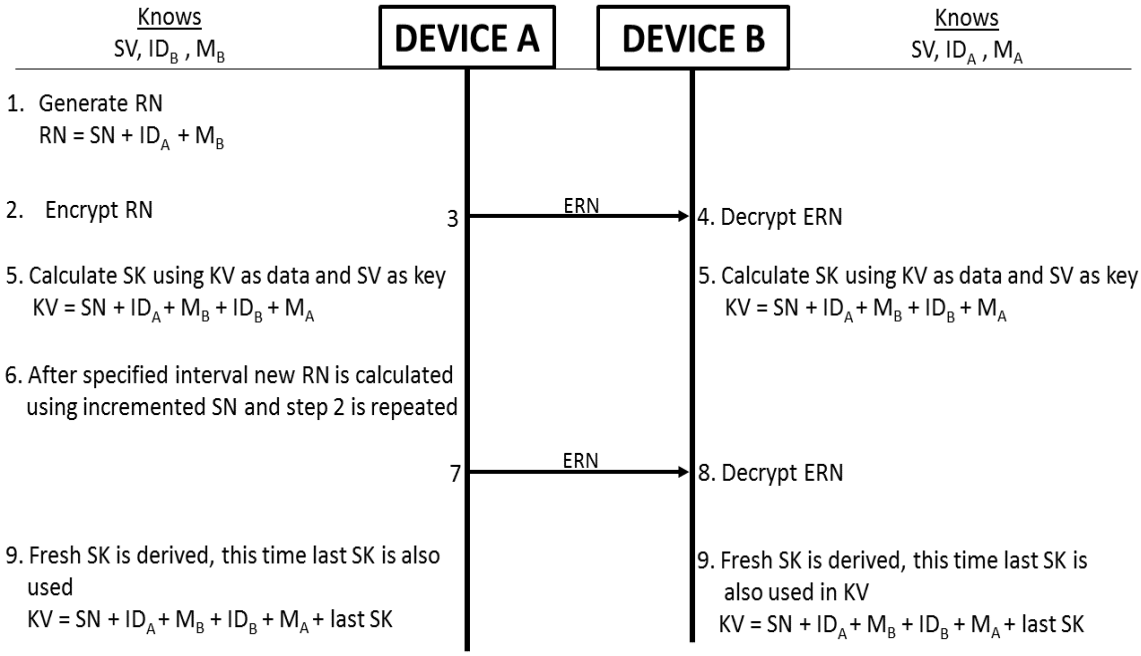

Figure – 9.2: Light Weight Key Establishment Framework using OOB Channel.

1) SV is shared among devices on OOB channel. At this stage both the device 'A' and 'B' knows following: -
   - SV
   - ID of each other.
   - MAC address (M) of each other.
2) Device 'A' acting as initiating device generate Sequence Number (SN).
3) Device 'A' generates RN which comprises of SN, ID_A and M_B. Contents of RN are concatenated in sequence and separated by symbol " , " and becomes: -

   SN, ID_A , M_B

4) RN is encrypted using SV as key and RN as data to lightweight encryption algorithm as shown in figure 9.3. Device 'A' then send encrypted RN (ERN) to Device 'B'.

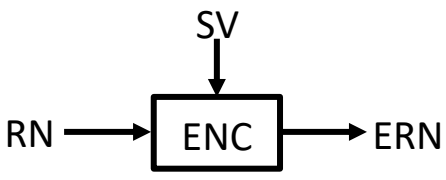

Figure – 9.3: Encryption of RN

5) After sending ERN to Device 'B', symmetric key that is SK is calculated by Device 'A' which will then be used for end to end security. For derivation of SK, Device 'A' uses Key Value (KV) containing SN, $ID_{A,}$ $ID_{B,}$ M_A and M_B. The KV is fed to ENC as data and SV as key for SK as shown in figure 9.4.

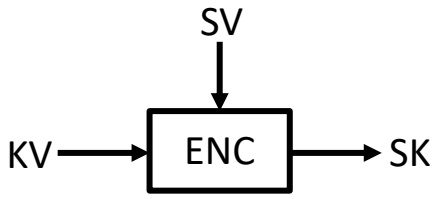

Figure – 9.4: Derivation of SK

6) Device 'B' receives encrypted RN, which is then decrypted using SV as shown in figure 9.5. After decryption, Device 'B' has the SN which will then be used for derivation of SK.

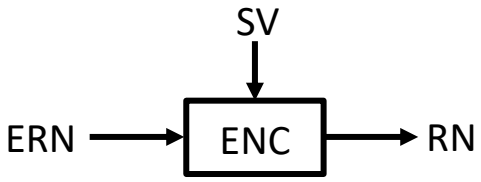

Figure – 9.5: Decryption of RN

7) Device 'B' has the SN, now it will generate symmetric key that is SK as calculated by Device 'A' (explained at step 5)
8) After specified interval of time, Device 'A' increment the SN to refresh SK. This time last SK is also used in KV. The new KV contains incremented SN, $ID_{A,}$ $ID_{B,}$ M_A, M_B and last SK. The process is again repeated as explained above to derive fresh symmetric key.

9.3.1.2 Analysis of Proposed Framework

A fundamental rule for encryption is that the encryption algorithm must not be kept secret instead remain available for evaluation. However, it is the encryption key which should be kept secret at all cost to avoid security breach. Analysis of proposed framework is as under: -

- Security of generated symmetric key is dependent on OOB channel.
- Security of calculated Secret Key is compromised, if Common Secret Value is exposed to attacker.

- Secret Key freshness is maintained after specified interval of time. In other words, new key is generated after specified time so as to avoid using one key for longer duration.
- To generate fresh Secret Key, OOB channel is not required for exchange of Common Secret Value. However, incremented Sequence Number and already operational Secret Key along with other parameters are used for generation of new symmetric key.
- Incremented Sequence Number enables the device to verify correctness of received parameters and legitimacy of initiating device for generation of fresh symmetric key.
- Authentication is achieved in terms of encrypted Random Value sent to Device 'B'. Encrypted Random Value is decrypted by using Common Secret Value which includes parameter like ID of initiating device, MAC address of Device 'B' and Sequence Number thus creates trust on initiating Device 'A'.
- Initiating Device 'A' trust Device 'B' in a sense that it has Common Secret Value used to decrypt Random number for Secret Key derivation.
- This scheme can be implemented among devices and between central entity and device for end to end security.
- Selection of light weight algorithm and exchange of few parameters for Secret Key derivation do not consume resources thus suitable for IoT network.

9.3.1.3 Comparison of Proposed Framework with other Key Management Schemes

Effective key management is essential to the security of cryptosystem. There are various open source and proprietary methodologies are available for key management for security suits. Proposed framework has been compared with two mechanisms (ZLL and Bluetooth) to draw efficacy of key management.

- **ZLL**. The security of ZLL protocol is based on global master key and do not require OOB channel. The ZLL master key is provided to every certified manufacturer and bounded with Non-Disclosure Agreement (NDA). This global master key is preconfigured in every device which is then used to encrypt and decrypt network key for secure communication. In case, ZLL master key is revealed by insecure product or extracted by any mean; then the secret key will not remain secret any more. Secondly, once the network key is derived from global master key

then it is not refreshed and remains unchanged. However, proposed framework does not mandate preconfigured master key instead shared among entities by using OOB channel. Based on shared secret value, the encryption key is derived for both the device. Moreover, generated secret key does not remain constant but change after specified interval to maintain key freshness.

- **Bluetooth Standard Pairing Protocol**. In standard pairing protocol, secret PIN is exchanged using OOB channel and used for derivation of link key for security. However, proposed framework also utilizes OOB channel for derivation of secret key but it also provides mechanism to refresh secret key which is not specified in Bluetooth standard pairing protocol.

9.3.2 Proposed Light Weight Key Establishment Framework Involving Trusted Third Party

In this proposed framework, session key is established for client to access IoT device. On the other hand, constrained IoT device calculate the "Secret Key" using Random number (provided by trusted third party) and Common Share Value. Three entities are involved in this framework which are as under: -

- **Constrained IoT Device**. Smart entities deployed in IoT network and have Internet access. These devices are constrained in terms of computation, power, memory and bandwidth therefore unable to perform PKI mechanism. These entities are registered with trusted third party and is provided with Common Secret Value prior to deployment in IoT network.
- **Client**. These are the entities who does not suffer from constrained resource and in possession of computing devices like laptops, smart mobiles, PDAs, tablets etc. Therefore, capable to perform resource heavy security mechanisms like IPSec, HTTPS and others. Client is the entity who wishes to access constrained IoT device.
- **Trusted Third Party**. Prior to deployment, IoT devices are registered with third party where Common Secret Value is shared among them. Similarly, legitimate clients are also registered with third party. Trusted third party also provides flexibility in terms of adding new devices and clients after IoT deployment and to change Common Secret Value at any stage. Trusted third party is an entity which contains repository of Common Shared Value associated with constrained IoT device and credentials of authorized clients.

9.3.2.1 Overview of Proposed Framework Involving Trusted Third Party

Client access IoT device and the authentication process invokes generation of session key for the client. The client is directed towards trusted third party which is running a web server. Client after authentication connects with trusted third party and request for session key required to establish secure connection with IoT device. In response, trusted third party provides Secret Key (session key) to Client over HTTPS and send few parameters to IoT device for derivation of Secret Key. Salient of proposed framework is as under: -

- Trusted Third party is bounded by Non-Disclosure Agreement (NDA) and running a web server.
- Trusted Third Party shares Common Secret Values (SV) with IoT devices and stores identity of each device (ID_T).
- Clients are registered with trusted third party utilizing username and password (PW_C).
- Client request trusted third party for Session Key (SK) over secure channel. In response, trusted third party generates Random number based on Sequence number (SN), ID_T and PW_C.
- Trusted third party generates SK and send to client. Meanwhile, SN and PW_C is encrypted using SV and send to IoT device. Selection of lightweight encryption algorithm (XYZ) is at the discretion of trusted third part and IoT vendor.
- IoT device decrypt the received SN and PW_C for derivation of SK.

9.3.2.2 Workflow of Proposed Framework Involving Trusted Third Party

Step by step workflow of key establishment framework among Client and IoT device involving trusted third party is as shown in figure 9.6. Detail is as under: -

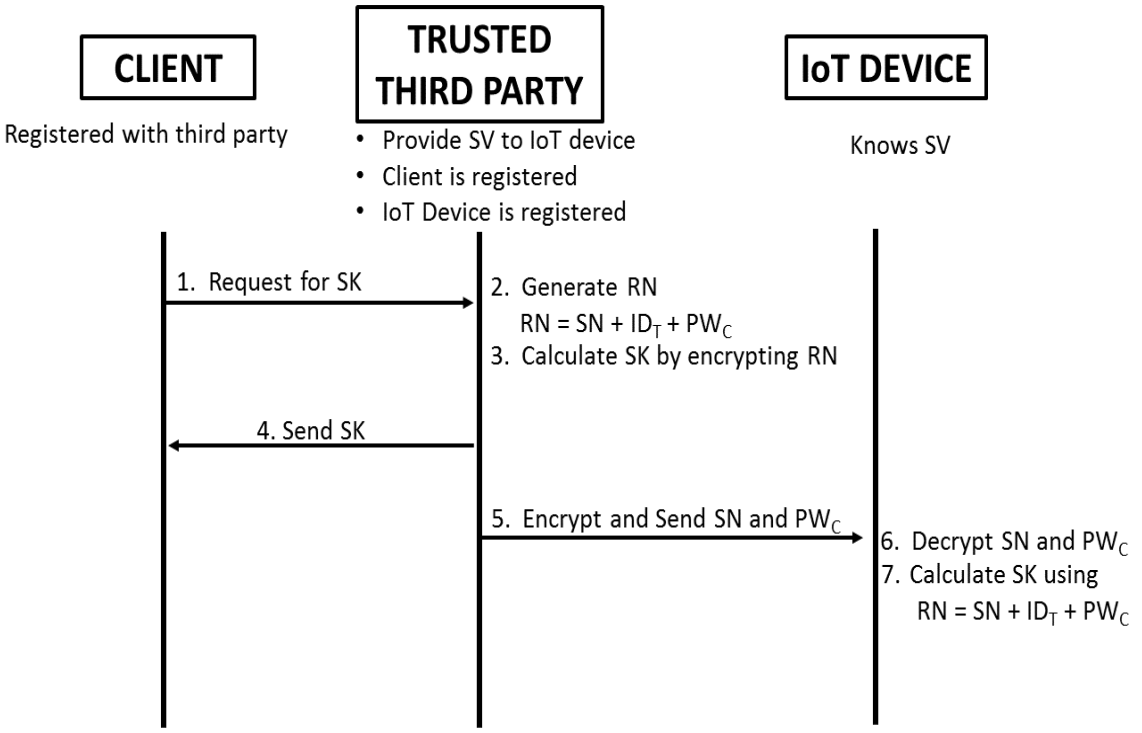

Figure – 9.6: Lightweight Key Establishment Framework involving Trusted Third Party

1) SV is allotted to IoT device by trusted third party during registration stage. So, both parties are in possession of SV.
2) Client access to IoT device invokes generation of session key for the client. The client is directed towards trusted third party and authenticate itself by using username and PW_C over a secure channel. After authentication client request for the SK required for security between Client and IoT device.
3) In response, third party server generates RN which consist of SN, ID_T and PW_C. RN is encrypted using SV as key and RN as data to lightweight encryption algorithm as shown in figure 9.7. The resulting value is the SK and send to client.

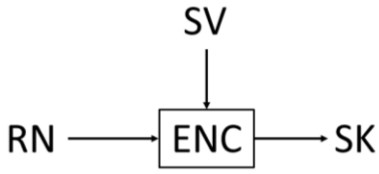

Figure – 9.7: Derivation of SK

4) After sending SK to client, third party server encrypts SN and PW_C as shown in figure 9.8. The encrypted value is sent to client for derivation of SK as SN, ID_T, PW_C is required.

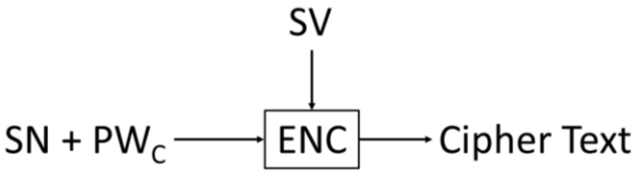

Figure – 9.8: Securing SN and PW_C

5) Upon receiving the encrypted value, IoT device decrypts cipher text as shown in figure 9.9 by using SV as key in order to retrieve SN and PW_C which is required in derivation of SK.

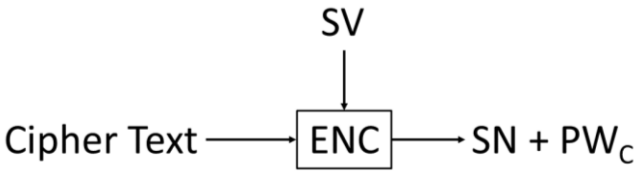

Figure – 9.9: Retrieving SN and PW_C

6) IoT device generate SK using RN which consist of SN, ID_T and PW_C. The RN is used as data and SV as key to lightweight encryption algorithm for generation of SK as shown in figure 9.10.

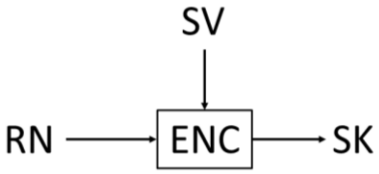

Figure – 9.10: Derivation of SK

7) Now, both Client and IoT device have symmetric key “SK” for end to end security.
8) After termination of established session between client and IoT device, the SK gets expired. For next session, fresh key will be generated with incremented SN by following the same process explained above.

9.3.2.3 Analysis of Proposed Framework Involving Trusted Third party

In this framework, three entities are involved where different parameters are used to derive secret key for security between client and constrained IoT device. Based on workflow explained above, analysis of proposed framework is as under: -

- Security of protocol is dependent on SK shared by IoT device and third party server.
- SK is valid for the session only; new key is generated after termination or expiry of session thus freshness of key is maintained.
- To protect RN when send to IoT device over unsecure channel, it is encrypted by third party using SV.
- This framework does not involve PKI mode therefore not heavy on resource constrained IoT environment.
- Trust is achieved among entities due to RN which contains SN, ID_T and PW_C.

9.3.2.4 Comparison of Proposed Framework and PKI

In existing PKI mechanism, trusted third party is involved and termed as Certification Authority (CA) who provides certificate to entities after necessary verification. Public and private key are assigned to verified entity for security. On the other hand, proposed framework also includes trusted third party but does not issue certificate to entities instead generate secret key and send to client. For IoT device, it sends requisite parameters for generation of secret key. Based on parameters, both client and constrained device have symmetric key for security mechanism. Hence, following are the advantages of proposed framework: -

- Does not involve certificates for entities, thus avoids overhead pertaining to certificate management in IoT environment. After expiration of certificate, it would be very challenging to withdraw expired certificates from large number of smart devices.
- Proposed framework is not resource heavy for highly constrained devices as compared to PKI mode which requires sufficient resources for implementation.

9.4 Proposed Model for Centralized Approach of IoT Network Deployment

Primarily, centralized and distributed approach can be utilized to deploy IoT devices in a network. In Centralized approach, client / server architecture is employed where central entity acts as intermediary device with which IoT devices are connected for data exchange and there is not much support available to directly access IoT entity. Alternatively, in a distributed or decentralized approach; collected data and related services are offered from edge of the network where various devices and applications in a network collaborate with each other dynamically. Both of these deployment

approaches have their own advantages and disadvantages; however, security controls and solutions are easier to implement in centralized approach which has been explained in chapter 4. Motivated by ease of security implementation and other mechanism in centralized IoT deployment, a networking model has been proposed in this section to achieve security and interoperability. The most significant component of proposed framework is a central device and named as "**Central Management Unit** (**CMU**)".

9.4.1 Central Management Unit (CMU) in Proposed Framework

CMU can be designed with enough resources to act as brain of the network by implement protocols and communication technologies necessary for interoperability, security and efficient network. The resulted devices can act as an intermediary device for smart devices, service provider, end user and to manage entire network at home or organization. CMU can be deployed to interconnect smart devices from different vendors thus creating its own network which can be accessed locally and remotely. CMU can provide control to end user for effective management of network and implementation of required security mechanism. Generated data will be received by CMU, which will then be processed into information and delivered it to its consumers. Accordingly, if client desires to use IoT services; he / she will make connection with CMU over the Internet after necessary authentication. Similarly, user from within the network can access CMU to receive notification and prescribed services. CMU acting as a single central device in a network with following feature can support dynamic functionalities: -

- High processing capability.
- Sizeable memory to store data provided by sensors and smart devices.
- RAM (volatile memory).
- Port for connectivity.
- Interfaces for out of band (OOB) channel.
- Different radio interface.
- 3G / 4G Connectivity
- User friendly GUI.

9.4.1.1 Recommended Technical Specification for CMU

Technical specifications can be selected as per the requirement of IoT network and available capital. Similarly, processing power and storage capacity can be adjusted according to requisite services and number of smart devices in IoT network. However, proposed specification for CMU is appended below but can be adjusted according to desired functionality: -

- Processor Speed: 3.7 GHz
- RAM: 4 GB
- Storage Capacity: 2TB
- Network Interface card
- WiFi and Bluetooth radio interface
- ZigBee radio interface
- Z-wave radio interface
- NFC radio interface

9.4.1.2 Cost – Benefit Analysis

Although cost benefit analysis is not in the scope of this research, but carried out very briefly to determine applicability of CMU in real world. Approximate cost of intelligent systems is US $1400 in order make smart home which includes smart lightening, smart climate control and smart security. Cost of CMU as per technical specification mentioned in section 9.4.2 is around US $335. These expected costs have been calculated on 15 October 2016 after consulting different online shopping sites and these quoted prices may vary. It is up to the choice of end user whether to make investment for security or not. Attaining security by spending US $335 is much more valuable compared to absence of any security mechanism and better network control.

9.4.1.3 CMU Functionality

Based on technical features, CMU as an intermediary device can perform functions for secure and effective IoT network. A resourceful gadget capable enough to address the challenges pertaining to IoT network. Prime functionalities of CMS are listed below: -

- To act as router where installed.
- To perform network address translation (NAT) functionality.
- Provides radio interface to accommodate devices using different frequency range.
- Ports, Near Field Communication (NFC) feature and other interfaces pertaining to OOB channel for pairing and key management.
- Ability to collaborate with other central entities for sharing of data and information.
- Capable to support and perform security and communication protocol.
- Provides interoperability among diverse smart devices.

- Ability to perform secure processing.
- Provides data security.
- Act as firewall, examining inbound and outbound traffic.
- Ability to maintain log.
- Provision of security by employing asymmetric encryption.
- Ability to perform symmetric encryption with smart devices within the network.
- Support protocols for secure key management.
- Provides notification based on received data to end user.
- Provides 3G / 4G connectivity.

9.4.2 Network Deployment by employing CMU

As CMU is designed to function as router and have different radio interfaces therefore various smart devices from different vendors can be deployed in a network using CMU. Moreover, CMU can be provided with the Internet connectivity thus can be accessed remotely and to connect with smart devices in a network. An intermediary device having installed protocols and with different radio interfaces, interoperability among various devices using different protocols and communication technologies can be achieved. Furthermore, various IoT service provider employs gateway in their smart solutions therefore CMU provides flexibility in terms of excluding vendor provided gateway or in extreme case the same gateway can be connected to CMU. In IoT perspective, CMU appears between smart devices and global Internet thus acting as a barricade between two domains for security purposes. CMU based network deployment is as shown in figure 9.11.

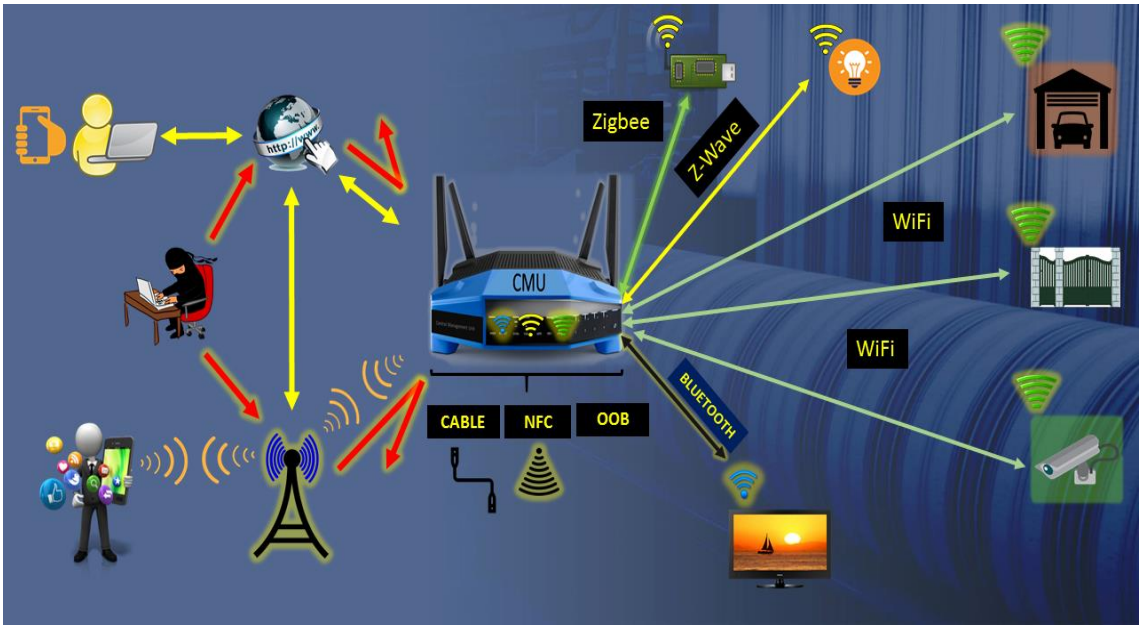

Figure – 9.11: CMU Based IoT Network

9.4.3 Access from Internet

CMU is a central entity having enough resources for data storage, processing and security mechanisms. All IoT devices are connected to CMU where collected data is send to CMU for processing and instructions are received from CMU for necessary action. Outside IoT network, devices are not visible instead CMU is accessible for data and requisite services as shown in figure 9.12. In order to access IoT network, entity has to authenticate itself to CMU. On successful authentication, CMU provides access for required purposes or services.

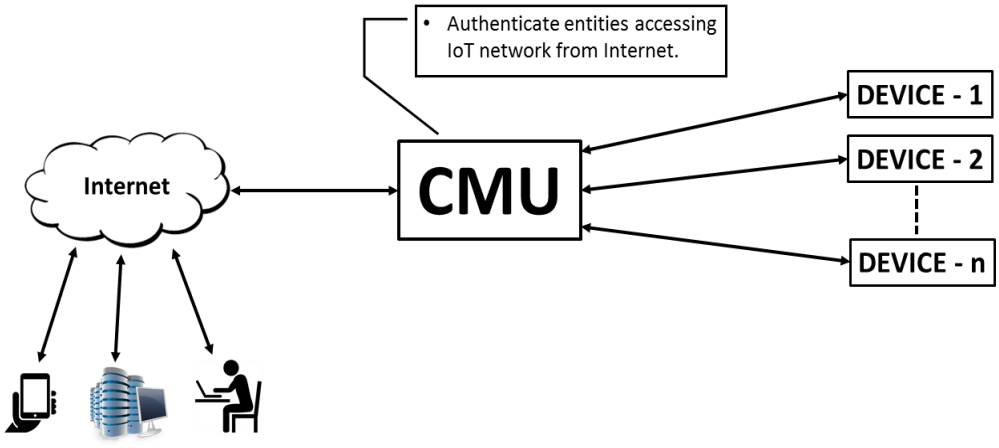

Figure – 9.12: Access from Internet

9.4.4 Access from within IoT Network

CMU is equipped with radio interfaces like WiFi, Bluetooth, and ZigBee therefore devices utilizing any of the said connectivity can connect to CMU. In this case, IoT devices are not directly accessible instead available via CMU as shown in figure 9.13. First, user has to authenticate itself to CMU and based on provided credentials the requisite access is granted. Once the identity and authentication parameters are created in CMU then for later use seamless connectivity can be provisioned to users.

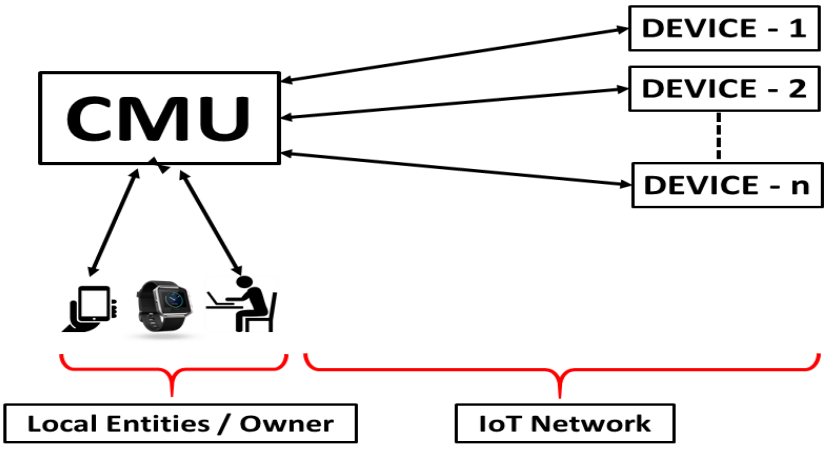

Figure – 9.13: Access from Within IoT Network

9.4.5 Identity Management utilizing CMU

IoT is a global network of interconnected smart devices. These devices deliver services and collaborate towards transformation of data into information / intelligence. Without robust security mechanism, attacks and malfunction can overshadow IoT benefits. Traditional protection mechanisms are difficult to implement in IoT architecture due to constraints such as processing capability, power availability, memory and bandwidth requirement. To address these challenges, it is important to understand the characteristics of IoT devices and the technologies which empower IoT vision. Following are the key points pertaining to IoT device: -

- **Presence**. Physical existence of device itself with communication technology.
- **Identity**. This distinguishes the device from other objects in a network.
- **Connectivity**. Smart devices communicate with other entities in IoT architecture. As a result, entities can access and locate each other for intended functionality.
- **Interactivity**. IoT devices interact and collaborate with others in heterogeneous environment. As a result, devices generate enriched intelligence and variety of services.

- **Dynamicity**. Interoperability, interaction and collaboration creates dynamic environment in which IoT device operates.

In this context, CMU acts as security gateway which do not allow direct interaction of devices and end users instead entities interact through CMU which provides secure functions. CMU can provide following capabilities for effective and efficient identity management: -

- An interface for implementation of identity management solution and software to cover identity of complete network at central location.
- Each attempt to access an entity invokes authentication process for which CMU can provide identity management.
- Devices collaborate with each other through CMU after verifying their identity to CMU. Credentials maintained at CMU can be used for federated identity management system.
- Authentication mechanism is linked to secure identification of IoT devices. CMU can provide the mechanism for secure verification of identity credentials. Each attempt to access an entity will invoke authentication process for which CMU can provide mechanism for identity management.
- CMU interface can offer device and owner identity while separating device from the owner to provide digital shadowing. Thus, enables the user's device to act on his behalf and ensures to address privacy concern.
- CMU can be designed to provide a platform for RFID system to verify identity of an object. RFID reader transmit signal to the tag attached with device and receive reflected signal can then be processed in CMU for identification.
- CMU can act as security filter where it checks the identity of consumer / object accessing the IoT network from internet. Likewise, device or entity will only associate to network if their identity is maintained at CMU thus avoiding association of rouge devices.

9.4.6 OOB Channels in CMU

In IoT network, there can be various devices with different mechanism to exchange master key for pairing and authentication thus availability of different OOB channel can bring flexibility in a network. In this regard, CMU can be designed to extend number of OOB channels as shown in table 9.1. Brief description of OOB channels which can be offered by CMU are as under: -

- **Physical Interface**. Cable connection and ports for the devices which requires physical connection.

- **NFC**. Near Field Communication (NFC) feature for the devices which relies on this type of OOB connectivity.
- **QR / Bar Code.** Devices with camera which requires to scan generated Quick Response (QR) or bar code can read the image from CMU interface for pairing or authentication.
- **Audio**. Those IoT devices which relies on audio for pairing or authentication can compare and verify the audio which is generated by CMU or vice versa.
- **Display and User Input.** Devices which uses display and input for pairing or verification can be employed in IoT network.
- **Input Only**. IoT devices with only input feature can view the value from CMU interface and feed the same using on board keypad.

Table – 9.1: OOB Channel

OOB Channels – CMU				
Pairing Methodology	**Equipment Capability**		**OOB**	**Procedure**
	CMU	**IoT Device**		
Physical Interface	• With Display • With Input feature • NFC connectivity • Built-in mic and speaker • Hardware ports	Port to connect cable	Cable	Both the devices are connected with cable
NFC		NFC enabled	NFC	Unique value exchange using NFC
QR / Bar Code		With camera	Visual	Scan QR/Bar code using camera
Audio		With built-in mic	Audio	Based on audio received, verify unique value
Display and User Input		With display and input feature	Visual	Compare the unique value and feed the value
Input Only		With keypad	Visual	Feed unique value using keypad

9.4.7 Pairing, Authentication and Authorization through CMU

Low cost wireless connectivity is allowing almost everything to get connected in LAN, WAN and around the globe. This connectivity is the driving factor for the success of IoT and forming network of networks. Security threat of current Internet is expected to rise due to high level of heterogeneity together with huge scale IoT systems where human, machine, devices and system interact among themselves. As IoT is characterized by its heterogeneous nature, challenges pertaining to security and privacy must be addressed at an early stage. Pairing, authentication and access control are the key areas for security of IoT architecture. It is highlighted that device pairing / authentication coupled with authentication and authorization of entities requires human intervention or "Out of Band (OOB)" channel, since IoT devices do not have prior knowledge about each other and are unable to differentiate legitimate and illegitimate entities via automated mechanism. Authentication or pairing process is based on identifying each other with distinctive set of credentials after which access is granted to authenticated entity.

In this proposed framework, CMU being a central controlling entity in a network can provide platform for pairing / association, authentication and authorization to avoid threats like tampering, eavesdropping, MITM, evil twin and others. Primarily, CMU can extend security mechanism to check connection from Internet, access from within the network and association of device to a network as shown in figure 9.14.

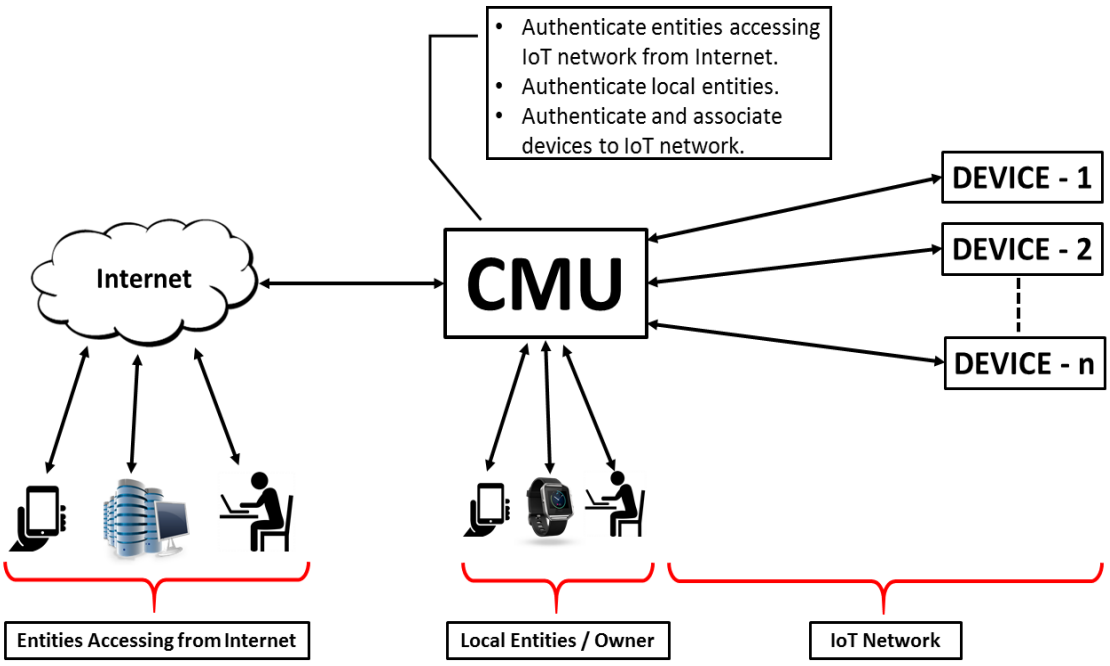

Figure – 9.14: Pairing, Authentication & Authorization at CMU

9.4.8 Scenarios for Authentication by using OOB Channel

9.4.8.1 WiFi Enabled Devices

CMU can act as access point (AP) for WiFi enabled devices where clients (IoT devices) authenticate themselves using pre-shared key (PSK). The PSK can be exchanged via OOB channel between smart device and CMU. PSK in conjunction with Service Set Identifier (SSID) set by CMU generate Pair Wise Master Key (PMK) for further computation of keys. Thus, CMU can authenticate a device based on PSK by employing OOB and creates a secure link between CMU and associated device as shown in figure 9.15.

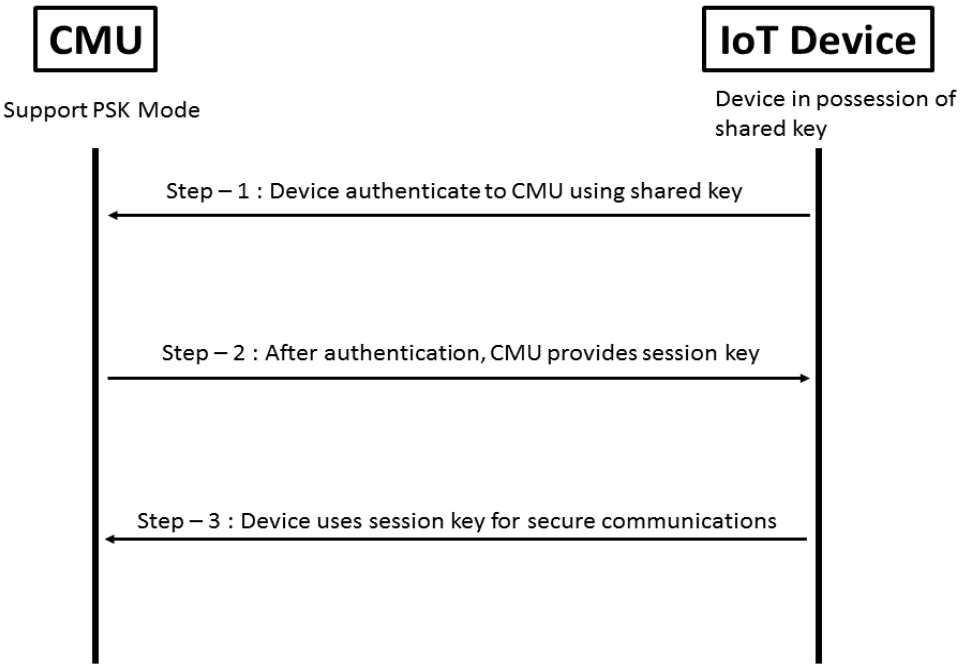

Figure – 9.15: Authentication Protocol for WiFi Enabled IoT Devices

9.4.8.2 Bluetooth Enabled Devices

Bluetooth device pairing allows two devices to authenticate each other and creates secure wireless connection. In this context, Standard Pairing Protocol for Bluetooth enabled IoT devices also needs OOB to exchange parameters. As discussed above, CMU can be designed for various OOB channel to exchange security parameter with IoT devices. Standard Device Pairing protocol is specified in Bluetooth core specification, where it allows /support to establish symmetric key for device authentication and secure communication. The device pairing process consist of authentication, generation of initialization key and generation of link key. CMU can act as

initiating device to start standard pairing session by sharing secret "PIN" via OOB channel. CMU and device, both knows the shared secret called as "PIN" and their addresses. CMU sends a random nonce to IoT device and both generate the initialization key as a function of PIN, nonce and Bluetooth address of CMU. The IoT device then sends a new random value to CMU which is then used to compute another value (challenge) as a function of initialization key and addresses of both devices. CMU send this value to IoT device, which it verifies for authentication. The process is repeated in reverse to achieve mutual authentication. The sequence of protocol is as shown in figure 9.16.

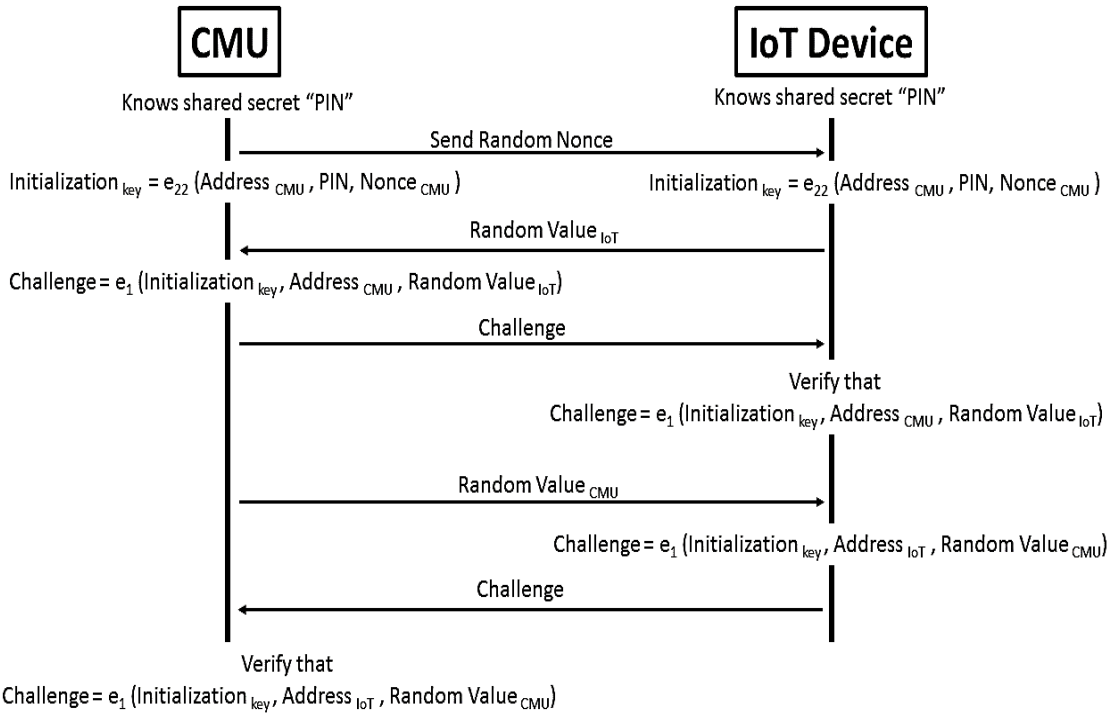

Figure – 9.16: Standard Pairing Protocol

9.4.9 Benefits of CMU Based IoT Network

Based on features and offered functionality, following are the benefits which can be provided by CMU: -

- Interoperability through APIs, application software and radio interfaces.
- Provides capability to control, manage and monitor IoT network.
- CMU will be able to collaborate with other remote entities for sharing of data and information.
- Vendor specific and proprietary service can be offered using CMU.

- Owner can control sharing of data received from smart devices.
- Capable to handle additional work load as CMU is not resource constrained.
- Additional hardware can be added to expand functionality.
- Better control over configuration management.
- Updating the firmware and patch management is efficient as CMU will allow only trusted traffic over the internet.
- Communication status or connectivity can easily be monitored.
- Segmentation of network can be done using CMU, thus centralized approach can take the form of distributed IoT network.

9.4.10 Disadvantages of CMU Based IoT Network

Following are the draw backs of CMU based network: -

- Adversaries strive for the target which offer immense benefit therefore CMU being the main component appears in this category.
- CMU can have suitable protection arrangements but any vulnerability can jeopardize the whole system or network.
- User involvement is another factor which can create misconfiguration due to limited expertise and may yield an opening for attackers to exploit the network.
- Centralized approached is a single point of failure as downtime, interruption, fault or malfunction of single device can cause damage to entire network.
- Adversary can also capture processed data, instead of raw data from a single entity.

9.4.11 Comparison of CMU and Similar Solutions

There are various platforms (gateway or hub) available for centralized IoT network deployment and many vendor offers IoT smart solutions employing central entity for connectivity of IoT devices. Features and functionalities suggested in CMU based IoT network can be employed for better efficiency, interoperability and security mechanism. Comparison of available IoT solution and CMU are as under: -

- **Philips Hue Smart Lightening System**. The lightening system comprises of at least one smart light which is connected to gateway or hub. The gateway is connected to Internet through home router via Ethernet of WiFi. In order to control the lights such as turning ON or OFF, changing brightness or color and to have remote access; application on mobile device is required to be installed. Consumer send the requisite command through their installed

application via Internet or home router to gateway which translates the received query for desired functionality. Philips employs ZLL protocol for their smart solutions and uses global master key for devices association thus lacking flexibility to incorporate foreign devices. Comparison between CMU and Philips Hue is enlisted in table 9.2.

Table 9.2: Comparison of CMU with Philips Hue

Features	**CMU based IoT Network**	**Philips Hue Smart Lights**
Radio Interface	WiFi, ZigBee, Z-wave and Bluetooth	WiFi and ZLL protocol
OOB	Yes	No
Interoperability	Yes	No
3G / 4G Connectivity	Yes	No
Firewall	Yes	No
Log Maintenance	Yes	No

- **Intel gateway Solutions for Internet of Things**. Intel offers family of platforms in the form of gateway for IoT in order to enables companies for seamless connectivity and data security [92]. Intel Gateway Solution for IoT provides building block to enable connectivity of legacy devices and latest smart object in IoT network. It allows integration of different protocols and technologies for networking, provides embedded control and offers robust security. Three series of Intel Gateway for IoT are available such as DK100 Series, DK200 Series and DK300 Series. Each type provides different form of features and functionality to form IoT network. The functionality of Intel Gateway can be enhanced by incorporation CMU's features and functionalities like various OOB channel, radio interfaces and NFC feature. Comparison between CMU and Intel Gateway for IoT is enlisted in table 9.3.

Table 9.3: Comparison of CMU with Intel Gateway

Features	CMU based IoT Network	Intel Gateway for IoT
Versions with different features	No	Yes (DK100, DK200 & DK300)
Radio Interface	WiFi, ZigBee, Z-wave and Bluetooth	WiFi, ZigBee and Bluetooth
OOB	Physical Interface, NFC, QR / Bar code, Audio, Display and User input	Without NFC and QR / Bar code
Interoperability	Yes	Yes
3G / 4G Connectivity	Yes	Yes
Firewall	Yes	Not mentioned
Log Maintenance	Yes	Yes

9.5 Security Guidelines for IoT

There are various building blocks of IoT, among many of them security is the one which is fundamental to its success. Security is not a onetime measure instead a continuous process which merits innovation and improvement to meet emerging challenges. Interactivity, interaction and collaboration of IoT devices increases the security challenges and attack surface for adversaries. One of the practical manifestation of increased attack opportunities has been seen on 21 October 2016 (Friday) where millions of hacked IoT devices were used to launch massive DDoS attack against major domain name system (DNS) provider called “Dyn” causing outage of many websites and services. IoT needs through planning before its implementation and security at every level because one or two secure layers are not enough to guarantee robust secure IoT implementation. In this regard, security guidelines for IoT at different layers are proffered below: -

9.5.1 Security at Human Level

IoT is the ecosystem of smart objects, sensors and actuators which interacts and offer diverse range of services. Prevention is the best methodology to avoid malicious incidents. The more the security policies are adhered, the more robust IoT security will be. Irrespective of IoT network architecture i.e. centralized or distributed; people are involved in designing, planning and implementation therefore needs to be security

aware to guard against malicious incidents. In this context, individuals are the key in security chain because it is the person who evaluates and implement appropriate security solutions. In this regard, following are the guidelines pertaining to individuals for secure IoT ecosystem: -

- **Training**. User awareness and training is the first step towards security. Best security practices enable how to achieve effective security in IoT network. Users and administrators must be made aware pertaining to strong passwords, turning off radio interface when not in use, reporting lost devices, secure configurations and falling for offers which appears legitimate.
- **Documentation**. Documentation is an effective method to trace IoT asset, analyze functionality and evaluate incidents. Document classification can be made on sensitivity of data so that suitable focus can be given to those which are more critical.
- **Reporting**. User friendly interface and channel to report vulnerabilities, threats or exploit helps in efficient management of IoT network and its related resources. In corporate or government offices, reward system can be introduced to inculcate initiative for reporting IoT related events, incidents or vulnerabilities.
- **Vendors**. Service providers must create mechanism to educate, inform or alert end users about latest security incidents, secure configuration and security updates. Short message service (SMS), web portals and email can be utilized to provide timely information.
- **Patch Management and Updates**. Users must verify patch, firmware or upgrades to avoid insecure implementation or to create backdoor in IoT network. User can check the source of the file that it is from trusted party, can scan the file for malwares and can check the integrity of file as well.

9.5.2 Security at Device Level

Device security is of paramount importance to guard against tampering, theft, failing and malfunctioning. Inadequately secured IoT devices not only have their local impact but can also harm globally which the world has witnessed in the form of DDoS attack on “Krebs on Security” and domains name system (DNS) called “Dyn”. Adversary can have physical access or remote access to exploit IoT device vulnerability. Instead of destroying device in IoT network, an attacker can draw the sensitive information or can create IoT botnet. Thus, security of IoT devices, gateway or controllers is critical issue and

very challenging. Moreover, absolute physical security cannot be achieved, however robustness of security can be increased by introducing multiple security features at all layers. Recommendation pertaining to device security is as under: -

- **Assessment**. Decision to implement device security depends upon the risk factor that a device can be compromised, the damage it can cause and the required resources to secure the device. In other words, if end user can not compromise on device security then it is justified to spend considerable resources for protection.
- **Embedded Security**. Designer and developer must also consider for embedded security so as not to expose consumer to potential harm.
- **Update / Upgrade**. Verify updates and patches before installing on IoT devices. Check how the file has been transported, scan the file, check its integrity and check the reputation that who is offering the file.
- **Default Settings**. Always change default pairing passwords, default authentication passwords and default security configuration.
- **Cabling**. If cabling is used for connectivity, then encase them in concrete or ducts to guard against tapping, MITM or eavesdropping.
- **Testing**. Test the device before deploying by using fuzz testing methods. Moreover, periodic testing must also be carried out to check the devices for their prescribed functionality.
- **Authentication Mechanism**. Effective authentication mechanism must be used such as two factor authentication or finger print and adopted mechanism must lock the device after three failed authentication attempts.

9.5.3 Security at Network Level

IoT ecosystem is characterized by its heterogenous nature which mandates security at network level. Security at network layer requires cryptographic algorithms and efficient key establishment mechanism along with security protocols for secure communication among devices. Advanced Encryption System (AES) may work in some IoT devices and may not be implementable in other IoT devices due to constrained resources. In IoT architecture, security mechanisms need to be smaller and faster with no reduction in security level. In this context, selection of symmetric and asymmetric algorithm requires detailed planning and assessment. From IoT perspective, thorough planning must be carried out at design stage and before deployment of IoT network. Moreover, security must be planned at all layers as secure mechanism at one or two layer is not

enough to achieve holistic security. Following are the guidelines for the security at network layer: -

- **Vulnerability Assessment**. Vulnerability assessment must be performed periodically to ensure that both credentials and authentication mechanism are according to prescribed policies. This may include password management, key management, periodic change of password and others.
- **Documentation**. Document all MAC addresses and identities of devices in the IoT network. This can be managed at central device or gateway so that IP assignment is carried out against documented devices. This helps in blocking unknown devices from accessing the IoT network.
- **Change Default Settings**. Disable guest account and default password of IoT devices. Attackers usually exploit default configuration for malicious activity.
- **Scan Open Ports**. Scan for open ports in all the devices especially in central entity or the edge devices connected with internet. Open ports provide easy path to adversary for exploiting IoT network.
- **Use of Different Service Set Identifier (SSID)**. IoT network employing more than one gateways or hubs then different SSID must be used instead using same SSID. This practice will enable network administrator to implement prescribed policies against each SSID allowing the organization to assign device to different SSID basing on their criticality and functionality. This type of network arrangement creates segmentation in the network which ensures that if one segment is compromised then other segments are safe from attacker.
- **Use of WPA2**. If using WiFi communication protocol, always use Wireless Protected Access 2 (WPA2) instead of Wireless Encryption Protocol (WEP) and Wireless Protected Access (WPA). WPA2 provides better security compared to other security protocols.
- **Firewall**. Firewall is the starting point when planning layered defense in IoT network. Central entity in the network can be used as host based firewall to filter inbound and outbound traffic based on type, port and destination.
- **Network Address Translation (NAT) Services**. Central entity or gateway in IoT network must be periodically check for misconfiguration. NAT is a protocol which has no built-in authentication mechanism and therefore trust all local entities thereby allowing rouge device to create hole through firewall.

- **Antivirus Software**. Updated antivirus can be installed in unconstrained IoT devices to safeguard against malicious programs. Moreover, antivirus programs can be used in gateways or central entity which act as intermediary device between IoT network and Internet.

9.5.4 Preventive Measures to become IoT Botnet

A zombie is a compromised smart device controlled by attacker. Zombie interacts and collaborate with other zombies to form "Zombie Army" called as "Botnets". The word botnet is a combination of two words "robot" and "network". Botnets are the collection of compromised smart devices which are controlled and instructed to carry out malicious activity. Following are the guidelines to avoid becoming part of botnet: -

- Do not click on suspicious link.
- Avoid downloading any files, software, patches or attachments which have not been requested or asked.
- Use of antivirus, firewall or IDS from trusted party helps to avoid malicious activity.
- Keeping the installed software and firmware updated can help to block attack vectors targeting the system.
- Vendors and manufactures deliver devices with default password and configuration. These default settings and password must be changed before deploying them in a network. Moreover, implement login limiting attempts in those devices which have enough computational resources.
- Secure and strong authentication mechanism helps to safeguard against attacker accessing smart device. Two factor authentication is one of the effective method to ward off attacker.
- Use security protocols such as DTLS, CoAPs, HTTPS, encryption algorithm and others to avoid security breach.
- Security gateway or central entity with robust security mechanisms can be employed in IoT network. This will act as barricade and stops internet born hacking attempts.

CHAPTER 10
CONCLUSION AND FUTURE WORK

10.1 Conclusion

IoT is the evolution of Internet which is seizing a gigantic leap to collect, analyze and distribute data which can then turn it into information, eventually into wisdom. So, it is smart devices and their interconnectivity which are the core components of IoT. IoT network can be categorized as Personal Area Network (PAN), Local Area Network (LAN) and Wide Area Network (WAN) where different smart objects interact with each other for their intended operation. The concept of IoT is to meet human needs by customizing the sensors or devices placed within a network, so that they can autonomously send important notifications on occurrence of an event. Likewise, connected objects automatically performing preset operation based on predefined criteria without human intervention. The potentials of IoT are limitless, the most fascinating phenomenon materializing within the cyber space. IoT has its application in all fields of life and has bright future prospects in term of adoption. So, in coming years the internet will see a huge growth in interconnected devices but with this growth cyber-attack surface will also rise as compared to present day cyber world. This highly interconnected network of smart devices will bring along and create more security challenges for IoT devices and the networks in which they operate. The major concerns pertaining to IoT devices are security and privacy which needs to be dealt from design stage. An important aspect of IoT ecosystem is its constrained resources in terms of processing, power, memory and bandwidth. Implementation of traditional security solutions and protocols are challenging and not always applicable in IoT ecosystem due to limitation of resources. Hence, security in IoT requires detailed assessment and planning to create balance between security mechanism and intended operation.

In this research, IoT has been discussed, explained and analyzed from different angles. This study is based on analytical research where security remained the primary focus to analyze various aspect of constrained IoT ecosystem. Various challenges especially security concerns are described with a view to highlight areas for improvement, optimization and deployment of new solutions to address issues pertaining to IoT. This thesis has proposed solutions to IoT challenges which includes design consideration for

developers and manufacturers to achieve security. Secondly, two frameworks for key establishment scheme are proposed for resource constrained IoT devices. Motivated by the analysis of IoT deployment approach carried out in chapter 4, a model based on centralized approach has been suggested to secure IoT network. Finally, guidelines for security at different layers have been recommended.

10.2 Future Work

IoT is an evolving technology in terms of optimized protocols, standards, communication technologies and security solutions. Unlike regular computing systems, IoT ecosystem is constrained in terms of processing, power, memory and bandwidth capacity due to which implementation of traditional security mechanism are challenging, difficult and not always applicable. Research community all around the world is contributing to address issues and security concerns in IoT domain. Meanwhile, several challenges still remain for IoT which merits research and development to reap potential benefits of IoT technology. Hence, IoT is a domain where various research areas are open and many of the researches are in full swing to address challenges for the success of IoT.

In this research, various aspect of IoT have been studied and analyzed. It is expected that security analysis of deployment approaches, protocols and IoT products can contribute towards research community interested to optimize, improve or develop new solutions to address security concerns in IoT. Moreover, IoT standardization has also been discussed where the impact analysis of IoT standardization has been carried out and proposal are proffered for unified standardization. As standardization contribute towards success of any technology; therefore, different aspect described and analyzed in this thesis can further be improved for IoT. Finally, solutions to challenges in IoT have also been recommended which can be evaluated and experimented for improvement.

References

[1] Karen Rose, Scott Eldridge, Lyman Chapin, “The Internet of Things: An Overview - Understanding the Issues and Challenges of a More Connected World”, The Internet Society (ISOC), 2015.

[2] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, “Internet of Things (IoT): A Literature Review”, Journal of Computer and Communications, 3,164-173, 2015.

[3] “Internet of Things Research Study”, HP Report, 2015.

[4] Wikipedia “Internet of Things”, Available: https://en.wikipedia.org/wiki/Internet_of_things

[5] “IoT European Research Cluster (IERC) on Internet of Things”, Available: http://www.internet-of-things-research.eu/about_iot.htm

[6] Recommendation ITU-TY.2060(06/2012) “Overview of the Internet of things”.

[7] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications” IEEE Communication Surveys & Tutorials, Vol. 17, No. 4, 4th Quarter 2015.

[8] Business Insider Tech Report, 2016, “Here are IoT trends that will change the way businesses, governments, and consumers interact with the world”. Available: http://www.businessinsider.com/top-internet-of-things-trends-2016-1? IR=T.

[9] Verizon Report, 2016, “State of the Market: Internet of Things 2016”. Available: http://www.verizon.com/about/our-company/state-of-the-market-int ernet-of-things.

[10] Yogesh Kumar Fulara, “Some Aspects of Wireless Sensor Networks”, International Journal on AdHoc Networking Systems (IJANS) Vol. 5, No. 1, January 2015.

[11] Resul Das, Gurkan Tuna, “Machine-to-Machine Communications for Smart Homes”, International Journal of Computer Networks and Applications (IJCNA), Volume 2, Issue 4, 2015.

[12] Ahmed Banafa, “IoT Standardization and Implementation Challenges”, 2016. Available: http://iot.ieee.org/newsletter/july-2016/iot-standardization -and-implementation-challenges.html. 2016.

[13] Carles Gomez and Josep Paradells, “Wireless Home Automation Networks: A Survey of Architectures and Technologies”, IEEE Communications Magazine, 2010.

[14] B. B. Olyaei, J. Pirskanen, O. Raeesi, A. Hazmi, and M. Valkama, “Performance comparison between slotted IEEE 802.15.4 and IEEE 802.1lah in IoT based applications,” in Proc. IEEE 9th Int. Conf. WiMob, pp. 332–337, 2013.

[15] M. Khanafer, M. Guennoun, and H. T. Mouftah, “A survey of beacon enabled ieee 802.15. 4 mac protocols in wireless sensor networks,” IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 856–876, 2014.

[16] Aiman J. Albarakati, Junaid Qayyum, Dr. Khalid A. Fakeeh, “A Survey on 6LowPAN & its Future Research Challenges”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue, 2014.

[17] Belghachi Mohamed, Feham Mohamed, “QoS Routing RPL for Low Power and Lossy Networks”, International Journal of Distributed Sensor Networks, Volume 2015, Article ID 971545,2015.

[18] T. Kothmayr, C. Schmitt, W. Hu, M. Bruenig, and G. Carle. “A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication”. In Proc. of IEEE SenseApp, 2012.

[19] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Jesus Alonso-Zarate, “A Survey on Application Layer Protocols for the Internet of Things”, Transaction on IoT and Cloud Computing, 2015.

[20] Shuang Song, Biju Issac, “Analysis of Wifi and Wimax and Wireless Network Coexistence”, International Journal of Computer Networks & Communications(IJCNC) Vol.6, No.6, 2014.

[21] Bluetooth SIG. Bluetooth Specification Version 4.0, 06 2010.

[22] Matti Siekkinen, Markus Hiienkari, Jukka K. Nurminen, Johanna Nieminen,” How Low Energy is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4”, IEEE 978-1-4673-0682-9/12, 2012.

[23] “Z-Wave devices and standards," Available: http://www.z-wavealliance.org/

[24] Minela Grabovica, Drazen Pezer, Sryan Popiu, Vladimir Knezeviu, “Provided security measures of enabling technologies in Internet of Things (IoT): A survey”, IEEE 978-1-5090-2957-0/16, 2016.

[25] Hussein Ahmad al-Ofeishat, Mohammad A.A.Al Rababah, “Near Field Communication (NFC)”, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, 2012.

[26] Yunjung Lee, DoHyeun Kim, “Threat Analysis, Requirements and Considerations for Secure Internet of Things,” International Journal of Smart Home, Vol. 9, No. 12, pp. 191-198, 2015.

[27] S. Krco, B. Pokric, and F. Carrez, “Designing IoT architecture(s): A European perspective,” IEEE WF-IoT, pp. 79–84, 2014.

[28] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges,” 10th International Conference FIT, pp. 257–260, 2012.

[29] Z. Yang et al., “Study and application on the architecture and key technologies for IOT,” ICMT, pp. 747–751, 2011.

[30] M. A. Chaqfeh and N. Mohamed, “Challenges in middleware solutions for the Internet of Things,” International Conference. CTS, pp. 21–26, 2012.

[31] A. Dunkels, B. Gronvall, and T. Voigt, “Contiki—A lightweight and flexible operating system for tiny networked sensors,” 29th Annual IEEE International Conference Local Computer Network, pp. 455–462, 2004.

[32] P. Levis et al., “TinyOS: An operating system for sensor networks,” Springer-Verlag, pp. 115–148, 2005.

[33] Q. Cao, T. Abdelzaher, J. Stankovic, and T. He, “The LiteOS operating system: Towards Unix-like abstractions for wireless sensor networks,” International Conference IPSN, pp. 233–244, 2008.

[34] E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, “RIOT OS: Towards an OS for the Internet of Things,”. IEEE Conference INFOCOM WKSHPS, pp. 79–80, 2013.

[35] X. Xiaojiang, W. Jianli, and L. Mingdong, “Services and key technologies of the Internet of Things,” ZTE Commun., Shenzhen, China, vol. 2, p. 011, 2010.

[36] C. Bormann, M. Ersue, and A. Keranen, “Terminology for Constrained Node Networks,” IETF, RFC 7228, 2014.

[37] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, “Security of the Internet of Things: perspectives and challenges”, Springer Wireless Netw DOI 10.1007/s11276-014-0761-7, 2014.

[38] Mario Weber, Marija Boban, “Security challenges of the Internet of Things,” IEEE, 2016.

[39] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Elsevier, Computer Networks 76, 146-164, 2015.

[40] Cahit Akin, “IoT: Centralized Vs. Distributed Architectures,” Information Week Network Computing, Available: http://www.networkcomputing.com/networking/iot-centralized-vs-distributed-architectures/435583941, 2015.

[41] Y. Saied, A. Olivereau, D. Zeghlache, M. Laurent, “Trust management system design for the internet of things: a context-aware and multi-service approach,” Elsevier, Computer Security 39 (2013) 351– 365, 2013.

[42] Kun Yang, Domenic Forte, Mark M. Tehranipoor, “Protecting End Devices in IoT Supply Chain,” IEEE, 978-1-4673-8388-2, 2015.

[43] C. Perera, P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, P. Christen, “Mosden: An internet of things middleware for resource constrained mobile devices,” Proceedings of the Annual Hawaii International Conference on System Sciences, Washington, DC, USA, pp. 1053–1062,2014.

[44] Almudena Alcaide, Esther Palomar, Jose´ Montero-Castillo, Arturo Ribagorda, “Anonymous authentication for privacy-preserving IoT target-driven applications,” Elsevier, Computer Security 37 (2013) 111–123, 2013.

[45] P.N. Mahalle, P.A. Thakre, N.R. Prasad, R. Prasad, “A fuzzy approach to trust based access control in internet of things,” 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems, VITAE, NJ, Atlantic City, pp. 1–5,2013.

[46] Xian-Yi Chen, Zhi-Gang Jin, “Research on Key Technology and Applications for Internet of Things”, International Conference on Medical Physics and Biomedical Engineering, Elsevier, 2012.

[47] N. Koshizuka and K. Sakamura, “Ubiquitous ID: Standards for Ubiqui tous computing and the Internet of Things,” IEEE Pervasive Computin., vol. 9, no. 4, pp. 98–101, 2010.

[48] Omojokun G. Aju, “A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges”, International Journal of Computer Applications (0975 – 8887), Volume 130 – No.9, 2015.

[49] Gaetano Carlucci, Luca De Cicco, Saverio Mascolo, “HTTP over UDP: an Experimental Investigation of QUIC”, ACM 978-1-4503-3196-8/15/04, 2015.

[50] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, Jesus Alonso-Zarate, “A Survey on Application Layer Protocols for the Internet of Things”, Transaction on IoT and Cloud Computing, 2015.

[51] Lidong Zhai, Li Guo, Xiang Cui, Shuhao Li, “Research on Real-time Publish/Subscribe System supported by Data-Integration”, Journal of Software, Vol. 6, No. 6, 2011.

[52] “uIP (micro IP)”, Wikipedia. Availble: https://en.wikipedia.org/wiki/UIP_(micro_IP).

[53] Michael Kirsche, Roman Kremmer, “uIP Support for the Network Simulation Cradle”, Proceedings of the “OMNeT++ Community Summit, 2015.

[54] Kristofer S. J. Pister, Lance Doherty, “TSMP: Time Synchronized Mesh Protocol”, IASTED International Symposium Distributed Sensor Network, USA, 2008.

[55] K. Nagarathna, Jayashree D.Mallapur, “An Investigational Analysis of different Approaches and Techniques for Time Synchronization in Wireless Sensor Network”, International Journal of Computer Applications, Volume 103 – No.5, 2014.

[56] Emerson Process Management “Emerson Wireless Security, WirelessHART and WiFi Security”, Emerson Security White Paper, February 2016.

[57] Toivanen, T. Mazhelis, O & Luoma, “E. Network Analysis of Platform Ecosystems: The Case of Internet of Things Ecosystem. In: Software Business”. Springer International Publishing, pp. 30-44,2015.

[58] Ovidiu Vermesan and Peter Friess, "Internet of Things – From Research and Innovation to Market Deployment," Revers Publishers, ISBN: 978-87-93102-94-1, 2014.

[59] Ahmed Banafa, “IoT Standardization and Implementation Challenges”, 2016. Available: http://iot.ieee.org/newsletter/july-2016/iot-standardization -and-implementation-challenges.html. 2016.

[60] Ved P. Kafle, Yusuke Fukushima, Hiroaki Harai, “Internet of Things Standardization in ITU and Prospective Networking Technologies,” IEEE Communication Magazine-Communications Standards Supplement, pp. 0163-6804, 2016.

[61] S. L. Keoh, S. Kumar, and H. Tschofenig, “Securing the Internet of Things: A Standardization Perspective,” Internet of Things Journal, IEEE, vol. 1, no. 3, pp. 265–275, June 2014.

[62] Wikipedia Definition. Available: https://en.wikipedia.org/wiki/ Standard.

[63] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, “Standardized protocol stack for the internet of (important) things,” Communications Surveys Tutorials, IEEE, vol. 15, no. 3, pp. 1389–1406, Third 2013.

[64] Ekram Hossain, “Editorial: Second Quarter 2016 IEEE Communications Surveys and Tutorials”. IEEE Communications Surveys & Tutorials, Vol. 18, No. 2, June 2016.

[65] Vedat Coskun, Busra Ozdenizci and Kerem Ok, “The Survey on Near Field Communication”. Sensors, 15, 13348-13405, 2015.

[66] C. Wang, Z. Bi, and L. D. Xu, “IoT and cloud computing in automation of assembly modeling systems,” IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1426–1434, May 2014.

[67] Wikipedia, Thread (network protocol). Available: https://en.wikipedia.org/wiki/Thread_(network_protocol).

[68] B. B. Olyaei, J. Pirskanen, O. Raeesi, A. Hazmi, and M. Valkama, “Performance comparison between slotted IEEE 802.15.4 and IEEE 802.1lah in IoT based applications,” in Proc. IEEE 9th Int. Conf. WiMob, pp. 332–337, 2013.

[69] Isam Ishaq, David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman and Piet Demeester, “IETF Standardization in the Field of the Internet of Things (IoT): A Survey”. Journal of Sensor and Actuator Networks, ISSN 2224-2708, 2013.

[70] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, "A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities," IEEE Wireless Communications, vol. 20, no. 6, pp. 91- 98, December 2013.

[71] Wikipedia, AllJoyn. Available: https://en.wikipedia.org/wiki/AllJoyn.

[72] AllSeen Alliance. Available: https://allseenalliance.org/sites/default /files/pages /files/intro_to_alliance_10.14.15_0.pdf

[73] Recommendation ITU-T Y.2060, “Overview of the Internet of Things.”, 2012.

[74] Recommendation ITU-T Y.2067, “Common Requirements and Capabilities of a Gateway for Internet of Things Applications.”, 2014.

[75] Wikipedia, Industrial Internet Consortium. Available: https://en.wikipedia.org/wiki/Industrial_Internet_Consortium.

[76] Industrial Internet Consortium, Industrial Internet Reference Architecture. Available: https://www.iiconsortium.org/IIRA-1-7-ajs.pdf.

[77] Open Interconnect Consortium, Smart Home Device Specification, Open Interconnect Consortium (OIC) Std. SHDS, 2015.

[78] Wikipedia, Open Internet Consortium. Available: https://en.wikipedia.org/wiki/Open_Connectivity_Foundation.

[79] Hasan Derhamy, Jens Eliasson, Peter Priller and Jerker Delsing, “A Survey of Commercial Frameworks for the Internet of Things”. IEEE, 978-1-4673-7929-8, 2015.

[80] Apple, “HomeKit,” Available: http://www.apple.com/ios/homekit/

[81] R. Frank, W. Bronzi, G. Castignani, and T. Engel, “Bluetooth low energy: An alternative technology for VANET applications,” in Proc11th Annu. Conf. WONS, pp. 104–107,2014.

[82] J. Decuir, “Introducing Bluetooth smart: Part 1: A look at both classic and new technologies,” IEEE Consum. Electron. Mag., vol. 3, no. 1, pp. 12–18, Jan. 2014.

[83] E. Mackensen, M. Lai, and T. M. Wendt, “Bluetooth low energy (BLE) based wireless sensors,” in IEEE Sens., pp. 1–4,2012.

[84] OGC, Sensor Web Enablement Architecture, Open Geospatial Consortium Std. Available: http://portal.opengeospatial.org.

[85] FG M2M Deliverable D2.1, “M2M Service Layer: Requirements and Architectural Framework,” ITU-T Focus Group on M2M Service Layer, 2014.

[86] M. Rahman, B. Carbunar, and M. Banik, “Fit and vulnerable: Attacks and defenses for a health monitoring device,” CoRR, vol. abs/1304.5672, 2013.

[87] N. Dhanjani, “Hacking lightbulbs: Security evaluation of the Philips Hue personal wireless lighting system,” August 2013. Available: http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html.

[88] Mark Stanislav, Tod Beardsley, “HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities” Published in Rapid7, September 2015.

[89] Joakim Wesslen. Home automation – rf protocols. April 2012. Available at http://tech.jolowe.se/home-automation-rf-protocols.

[90] T. Zillner, “Zigbee exploited - the good, the bad and the ugly,” in Black Hat USA, 2015. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[91] “Identity Management”, Wikipedia. Available: https://en.wikipedia.org/wiki/Identity_management

[92] “Intel IoT Gateway Technology”, Avaialble: https://www-ssl.intel.com/content/www/us/en/embedded/solutions/iot-gateway/overview.html