Master Thesis

COMP9700A_COMP9700B_COMP9700C_COMP9700D

Submitted to the College of Science and Engineering in partial fulfillment of the requirements for the degree of Masters in Computer Science at Flinders University, Adelaide, Australia.

Topic: - Protection of personal information used by IoT devices in health care.

Name: - Rohan Taneja

Student id: - 2164777

Fan id: - tane0012

Supervisor: - Prof Trish Williams

Submission Date: - 5th November, 2018

Declaration

"I certify that this thesis does not incorporate without acknowledgement of any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person except where due reference is made in the text".

Abstract

The aim of this research is to explore IoT healthcare systems to understand the security concerns and identify secure architectures that can help address these concerns. The report explores the most common applications of IoT in healthcare such as healthcare monitoring and explores in depth the threats that are brought about from using this technology. It explains how security threats can affect the healthcare systems and patients as well as explores the consequences of the same. The research makes use of a secondary literature review based methodology to explore the solutions that are available to counter these threats. It also covers the details of some of the standards that are used in the IoT based healthcare systems for protection including ISO CD 30141 and ISO AWI 21823. IoT based secure healthcare architecture have been explored to understand what can help protect patient care systems from the security threats that arise from IoT network. Some of the architectures and methods details in the report include Elliptic Curve Cryptography, TinySec, Datagram transport Layer security, SEA architecture, and secure IoT architecture using body sensor networks. Based on the analysis of the secondary qualitative data found on the subject, certain recommendations have been made to be followed by organizations using IoT healthcare systems to make their systems secure.

TABLE OF CONTENTS

Chapter 1. Introduction

Since its inception, Internet of Things (IoT) technology has seen nothing but an uphill progress. Over the past decade the total number of connected devices has multiplied rapidly and the numbers are predicted to increase in future, too, as indicated by Figure 1. Figure 2 exemplifies the instrumental role that IoT plays in numerous walks of life; from healthcare to industries to defense, IoT is everywhere.

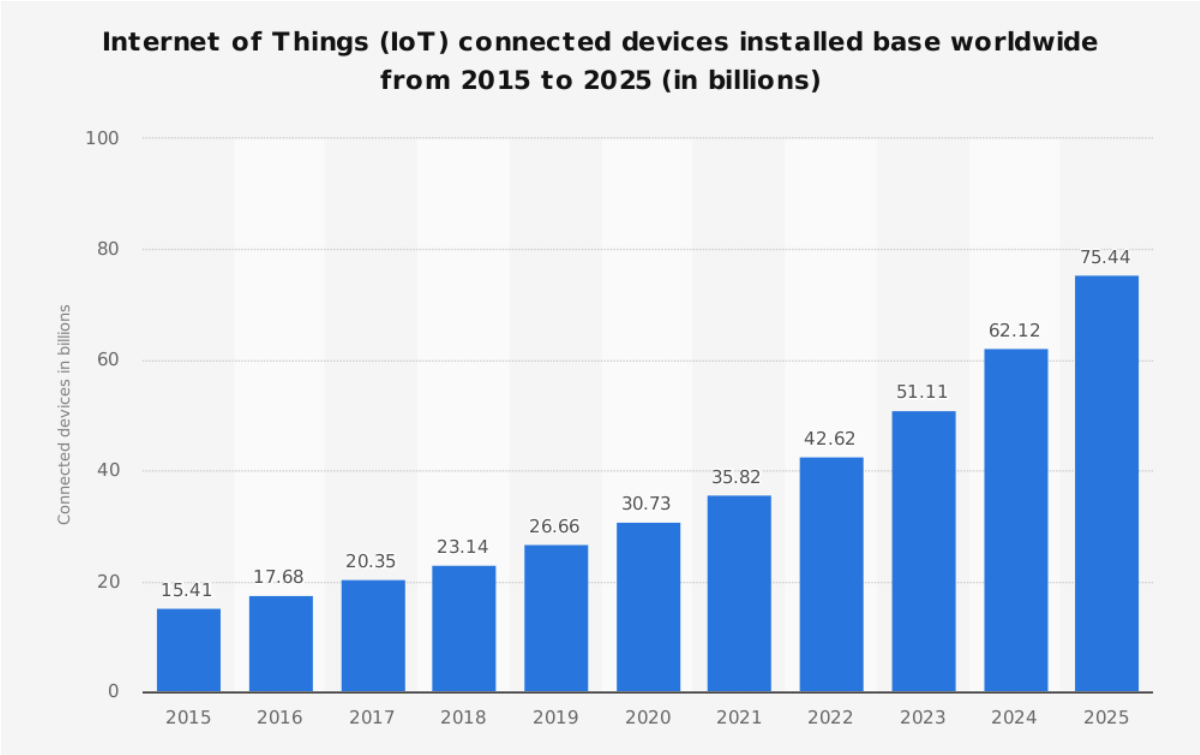

Figure 1: Statistics of IoT connected devices installed (Jain, 2018)

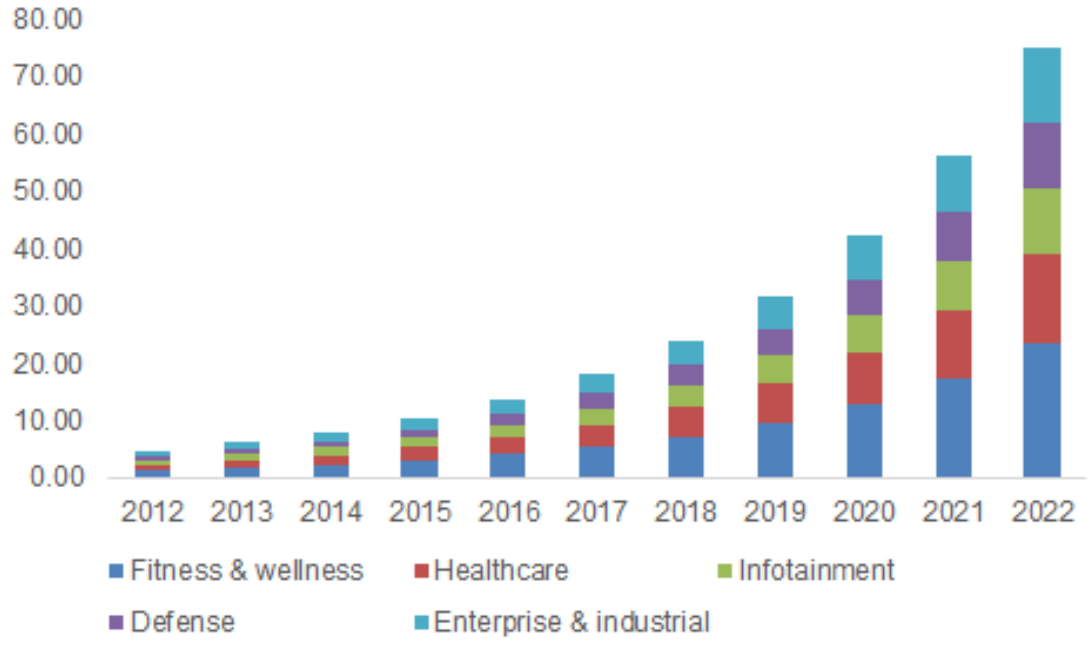

Figure 2: Contribution of IoT in different departments (Grandviewresearch.com, n.d.)

The aim of this research is to explore IoT healthcare systems and architectures to understand what security concerns are raised in these systems and what measures can be taken to overcome them. IoT devices involve physical objects that have sensors attached to them such that the data about the current activities of the object or the person to whom it is attached can be monitored through the use of a sensor and transferred to a remote server for further analysis. IoT devices feature an IP address to connect everyday objects to the internet, wirelessly and to enable this exchange of information (IoT Agenda, n.d.). Kodali, Swamy and Boppana, (2017) have given a very precise definition of IoT based healthcare in their conference paper 'An Implementation of IoT for Healthcare,' defining it as a platform where 'diverse distributed devices aggregate, analyze and communicate real time medical information to the cloud, thus making it possible to collect, store and analyze the large amount of data in several new forms and activate context based alarms.' In healthcare, the most common use of IoT is for healthcare monitoring of the patients who may be disabled or sick. It brings many benefits as tracking helps monitor and assess any potential hazards or coming diseases such that proactive steps can be taken by the healthcare practitioners to

prevent the patient from suffering any major problem. However, as the system connects devices to internet, a seamless network is created that also exposes the users or patients to the cyber related risks some of which are broadly classified in Figure 3.

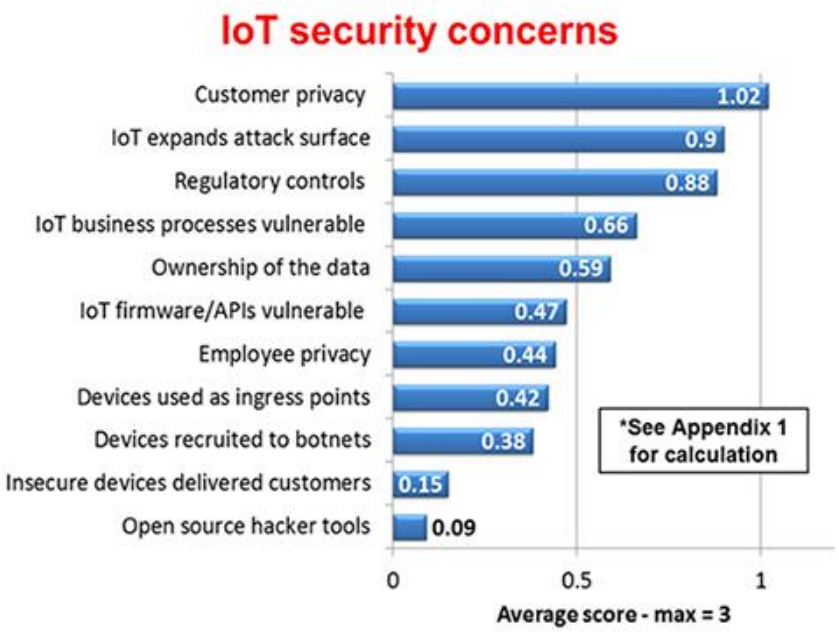

Figure 3: IoT related security concerns

This research would explore the health care systems and architectures of IoT to understand the data reliability and security concerns as well as conduct a critical analysis of the solutions that can help overcome the difficulties that occur due to security threats.

1.1 Aims & Objectives

The aim of this research is to explore the security and data reliability problems and solutions of health related IoT by exploring healthcare systems and architectures. To achieve this aim, some research questions are needed to be answered:

- How do IoT based healthcare systems work?
- What architecture can be used to secure healthcare IoT systems?
- What are the security concerns in the healthcare IoT systems?
- How is reliability of data ensured in IoT based secure healthcare systems?

- How can healthcare systems be made secure with the use of right IoT architecture?

1.2 Document Outline

This dissertation document is divided into five chapters, each addressing one major aspect of the research project.

Chapter 1 is an introductory chapter, introducing readers to the problem statement, relevant concepts and the aims and objectives of the research. Key questions that will be answered through the course of the document are also mentioned.

Chapter 2 discusses all the theoretical information about IoT and IoT in healthcare extracted from various sources, for example journals, research papers, conference papers, websites etc. The reader is familiarized with IoT architecture, components and some important applications, IoT based healthcare systems, their privacy and security issues and how they are addressed. Some security related standards are also mentioned

Chapter 3 is an overview of how the research is carried out and the main philosophies governing this process. The different steps related to the collection of information sources, extraction and analysis of data, limitations and interpretation are mentioned in this chapter.

Chapter 4 is solely based on the discussion of the data collected from different sources. It analyzes different IoT based health security systems for example, TinySec, Elliptical Curve Cryptography, Datagram Transport Layer Security and Body Sensor Network.

Chapter 5 concludes the dissertation with a brief discussion of the results and recommendations for future work in IoT. Some IoT based devices, expected to be released in the near future are also mentioned.

Chapter 2. Introduction to IoT in Healthcare and Relevant Definitions

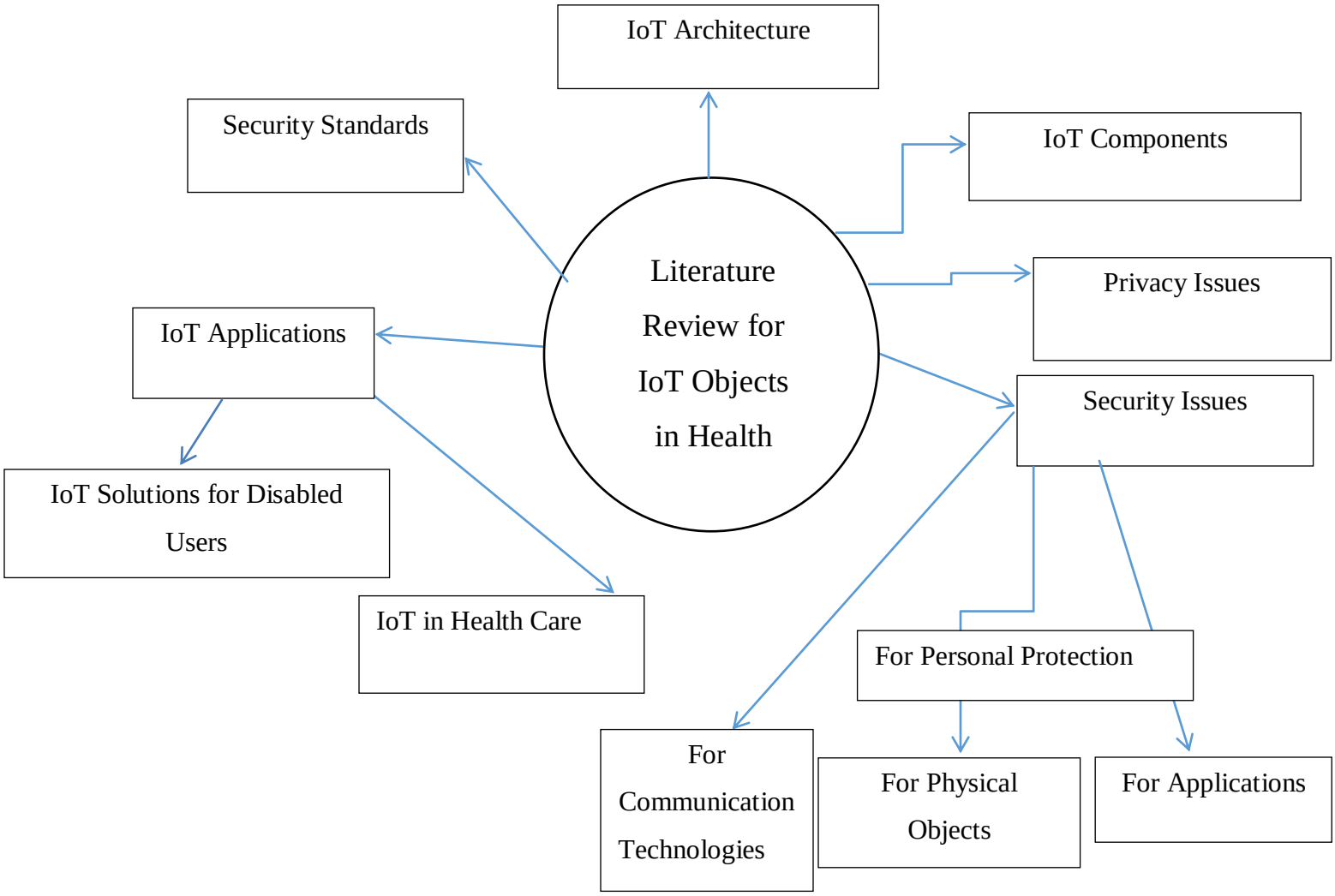

Figure 4: A graphical classification of IoT Objects and Standards in Healthcare

Internet of Things (IoT) is a dynamic distributed system of network of physical devices, vehicles and home appliances that can capture real world data through sensors, process the same to develop insights and communicate with others for sharing or exchanging these insights (En.wikipedia.org, n.d.). It has certain key characteristics that distinguish them from other networks and these include identification, communication, and interaction of anything that can include electronic devices as well as living beings (Kodali, Swamy and

Boppana, 2017). IoT devices can connect to the internet and perform these structured exchanges in real time (Collins, 2015). Connecting to internet also allows remote monitoring of the devices (Aroul, Walker and Bhatia, 2004). Many advanced and intelligent functionalities can be added in a device through it.

2.1 IoT Architecture

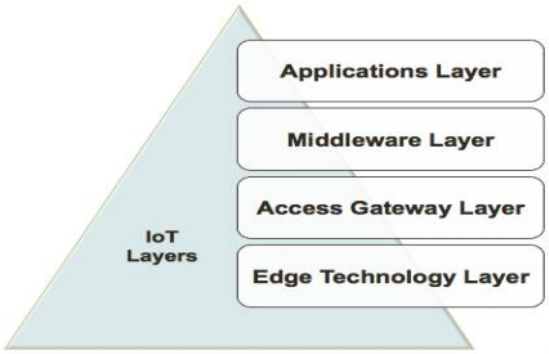

Figure 5: IoT layers (Rfwireless-world.com, 2016)

IoT architecture consists of four major layers that include edge technology, access gateway, middleware and application layer. The lower two layers involves capturing of data while the other two use the data captured for analysis and value addition (Bilal, A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers, 2017).

Edge Technology: It is the first layer of the IoT architecture that contains the hardware based data collection components like sensors, Radio-Frequency Identification (RFID) systems, Electronic Data Interchange (EDIs), Global Positioning Systems (GPS), cameras, and intelligent terminals. These components collect the information, processes it, and communicates the data to the next layer. RFID are the portable devices and has a reader tag and the data that is recorded is as per the need of the RFID tag. RFID tags are useful in enabling real time data monitoring. The data that is transmitted through the RFID tag can include information on devices and the patient in the case of patient monitoring system such

as glucose level, blood pressure, and location. IoT systems use Wireless Sensor Networks (WSNs) that having huge number of nodes that sense the results (Guth, et al., 2018).

Gateway: An access gateway handles the data received from the edge layer through technologies like Wi-Fi, Ethernet, Wireless Sensor Network (WSN), WI-Max, and Global System for Mobile Communication (GSM) (Carrez, 2013). The gateway enables sensors to connect with an external network via these technologies (Konsek, 2015). The gateway hardware pre-processes sensor data (filtering and aggregation) before sending it to a data center (Konsek, 2015).

Middleware: After the gateway comes the middleware, which is a software platform that provides a variety of data services including discovery, filtering, aggregation, analysis, and access control. The middleware connects the access gateway layer to the top layer, which is the application layer.

Application Layer: The application layer connects the IoT system to the users and it has two sub-layers including data management and application service. Data management layer provides services like directory, quality of service, cloud computing data, processing and M2M. Application layer includes an interface between the end users and the applications used in the enterprises (Uviase & Kotonya, 2018).

2.2 IoT Components

IoT has a variety of different components working together. One key component of the system is physical object that is used for collecting and monitoring information of the users. The data that this object or device would collect can include vital signs of health such as glucose levels, heart rate, and blood pressure (Grandviewresearch.com, n.d.).

Communication technology is another component, which serves as a link between the healthcare application and the devices. These technologies can be ZigBee, Bluetooth, Light Fidelity, or Wi-Fi. ZigBee is an IEEE 802.15.4 standard that works with low power and in short range (Radio-electronics.com, n.d.). The technology is built on Low Rate Wireless Personal Area Network (LR-WPAN) and operates in the 2.4GHz ISM band. Bluetooth,

which works on IEEE 802.15.1 standard also, operates in the same band but ZigBee costs less than Bluetooth. Bluetooth makes point to point or point to multipoint connections based on Wireless Personal Area Network (WPAN). Bluetooth devices can operate with low energies and thus, consume less power (Sidhu, Singh, & Chhabra, 2007).

Light Fidelity (Li-Fi) is a Visible Light Communication system and uses light unlike Wi-Fi, which uses radio waves. Rapid pulses of light between 400 and 800 THz keep being transmitted through an LED lamo, which is fitted on the transceiver. These LEDs transmit data in the form of light while the photoreceptors receive the signals and covert the same into the digital data. However, in the areas where there are obstacles such as walls and trees, Li-Fi cannot be used as the light transmitted can interfere with other sources of light such as sunlight or bulbs. The advantage of this technology is that it is a low cost technology and can eliminate the problem of overlapping of frequencies in signals so there is no electromagnetic interference. Li-Fi technology is used for patient monitoring within a room such as in the case of MRI scanner (Mallick, 2016).

Wi-Fi technologies include IEEE 802.11x Wireless LAN. These technologies work on three interoperable technologies including Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum (FHSS), and Infrared (IR). Wi-Fi standards like IEEE 802.11n perform well at the data rate of 600 Mbps under 2.4 GHz or 5 GHz Radio Frequency bands. The technology uses Multiple Input Multiple Output (MIMO) for maximum use of the band available. Protocols are available for security such as Wi-Fi Protected Access Points, Wi-Fi protected areas, Advanced Encryption Standard, and Wired Equivalent Privacy (Narendra, Duquennoy, & Voigt, 2015).

Long Term Evolution (LTE) is another Wireless broadband technology that uses 4G technology. This technology provides 75 Mbps of Uplink data rate and 300 Mbps of down Link data rate. LTE is very cost effective especially in the cases of M2M services. It can be used in healthcare for monitoring and tracking of patients and the devices attached to them. LTE-A is an actual 4G communication standard, which provides 3 GBps of downlink and 1.5 Gbps of uplink data rate at low latency. This technology also provided backward

compatibility with LTE networks and thus, services can take advantage of the LTE networks (Paavola, 2007).

2.3 IoT Applications

The application component in the IoT system takes care of organization and formatting of the data that happens across difference devices and IoT applications. Smart technologies are used for providing assistance to the users such as in smart home technology, where residents are assisted by the use of gadgets and equipment inside the home. Smart health systems can be used for helping people who are disabled by connecting them to the health practitioners through internet using IoT devices connected with their bodies. Wireless sensors can be put in clothes and other items used by a patient for enabling monitoring through IoT systems which allows for monitoring the patient behavior at the macroscopic level and identify any abnormalities in the behavior that could lead to a health problem for the patient. In such cases, the action can be taken remotely by a practitioner and alarm can be sent for initiating procedures for providing assistance (AL-mawee, Lilien, & Al-Fuqaha, 2012).

Smart Healthcare system users like doctors and healthcare providers can read the patient information through smart applications such as ECG data and diabetes status. Inputs can be provided in the real time through the use of sensors and RFIDs connected to IoT devices. Just like the bar-code on an ATM card, RFID powers up a chip or in this case a sensor with RF energy which returns an identification number. In the presence of an RFID a sensor can be used battery-free (eeNews Europe, 2016). The collected data is sent to cloud for storage and the data is then processed with cloud-based applications. Cloud storage allows data to be accessed from anywhere around the globe via the Internet. With the use of cloud computing, the costs of processing and management are reduced. This is because in the presence of cloud computing no technological equipment needs to be bought or maintained. Besides that, the cost of consulting services, installation of equipment and license agreements is cut off. The IoT system can use any of the deployment models from Software as a Service

(SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). IaaS involves a software and a hardware that takes service requests from users. PaaS tools enable cloud applications to be used for establishing control. SaaS can provide users services like storage, processing, and execution of applications (Bilal, 2012).

2.4 IoT in Healthcare

A variety of sectors including industrial and non-industrial make use of IoT devices for enhancing their infrastructure such as telecommunication, manufacturing, and healthcare. In the healthcare sector, the applications of IoT are on rise. It is used in healthcare services like m-health, assisted living, wearable, community healthcare, medical access, and embedded systems. M-health is an acronym for mobile health and involves the use of mobile technology for healthcare services. Some of the IoT applications are patient monitoring for ECG, Glucose level, body temperature, and oxygen saturation, and management of services like rehabilitation, medical management, wheelchair management, and smartphone devices (Bardach, Real, & Bardach, 2015).

Figure 6 given on the next page divides IoT based healthcare into two subcategories: services and applications. It gives a comprehensive overview of how IoT has influenced and aided healthcare provision. Services include a smart living, indirect emergency provision of health services, m-health, addressing drug reactions, securing and giving access to patient health information, wearable devices (Bardach, Real, & Bardach, 2015***)***. Applications are further divided into those targeted at an individual patient (single-condition) and those meant to cater to an audience (cluster conditioned) Single-condition applications include glucose level, ECG, blood pressure, body temperature and oxygen saturation monitoring (Bardach, Real, & Bardach, 2015***)*** while clustered-condition applications include rehabilitation systems, wheelchairs and smartphone healthcare systems

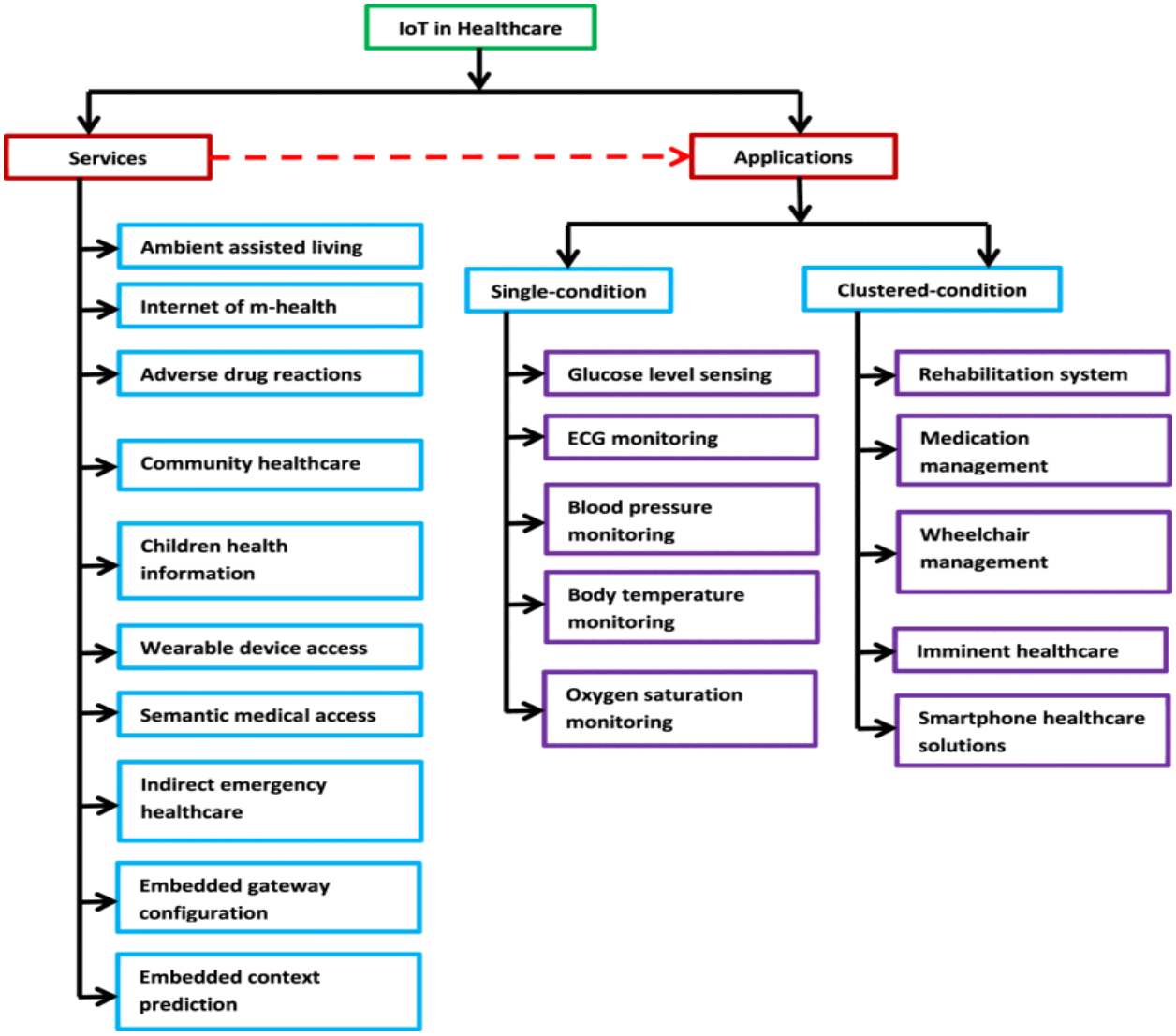

Figure 6: IoT in Health Care (Bardach, Real, & Bardach, 2015)

2.4.1 Health Care Systems

IoT has made it possible for health care systems to enhance their efficiencies in providing quality in cost effective ways such that quality services and more accurate diagnoses can be provided to the patients (infisim, n.d.). Patients and health care providers are establishing an automated communication between them such that the practitioner remains updated with the health status of the patient as well as can use smart healthcare

systems that have been built (Bardach, Real, & Bardach, 2015). This communication technology has been integrated in wearable devices like those used for glucose monitoring, blood pressure monitoring, oxygen level monitoring and body temperature monitoring (TechJini, 2017). Online patient health portals also allow patient information to be exchanged between different parties for example the patient and his/her doctors.

Smart healthcare systems involve capturing of human health parameters with biometric sensors. The communication happens between the patient and the healthcare practitioner or the caretaker though an IoT cloud (Bardach, Real, & Bardach, 2015).

Figure 7: The confluence brought about by the IoT (Bardach, Real, & Bardach, 2015)

Figure 7 shows a systematic diagram of how healthcare provision is made possible using IoT. Data is collected from patients via sensors, wearable devices, and m-health apps and fed to the IoT cloud. Doctors, medical practitioners and insurance companies extract this information to provide effective healthcare services for both treatment and prevention.

The benefits of using IoT devices over cloud include capture of real time data and making it more accessible for patients and healthcare service providers. A typical system of IoT in the healthcare sector includes a system to capture data, a cloud for connecting, and a health care portal (Neelam, 2011).

For example an IoT-based system would make use of a commercial microcontroller for example ATMega328P or NodeMCU mounted with a sensor as the device for sensing any attribute of the patient for example the body temperature of a patient. Once this device captures the data, it is stored in a database server such as MySQL, which is connected to a real time health portal that can be used for reviewing the health status of the patient. There are several Android based applications written using Java programming that can be installed on the mobile, table or a PC for accessing the real time data access portal. The system uses an Ethernet shield for providing the internet connection for real time data transfer between sensors and the database(West, 2016). Following are the different segments of an IoT-based healthcare system.

Data Acquisition: A sensor is used for capturing data from the patient or a healthcare unit. Some examples of these sensors are DS18B20 that is used for capturing heart beat values and microcontroller Arduino Uno ATmega 328P, which captures the body temperature data (Seo, Vairavan, Kulkarni, & Majure, 2013).

Cloud system: The data that is captured through sensing devices is transferred to a processor such as HLK-RM04 Serial through a Wi-Fi Module and gets stored in a MySQL server. This connection is established through an HTTP protocol (Goel, Srivastava, Pandit, Tripathi, & Goel, 2018).

Real Time Health Portal: a user through a healthcare portal that is usually written with Java and is made available through Android applications accessible through multiple devices including mobile laptops, tablets, and personal computers can view the data. An example would be an Android application that would give notification to a mobile user if any fluctuations is observed in the health of a patient (Abbasi, Memon, Syed, Memon, & Alshboul, 2017).

2.4.2 IoT Solutions for the Disabled Users

IoT solutions are used in a variety of healthcare services out of which providing support for the disabled is one in which IoT infrastructure is used for monitoring the patient suffering from a chronic ailment or some kind of disability (Kube et al., 2017). A lot of research has already been done in this area and thus, healthcare has seen many advances in the area. Understanding how these systems work can help exploring the possible applications of healthcare in the field.

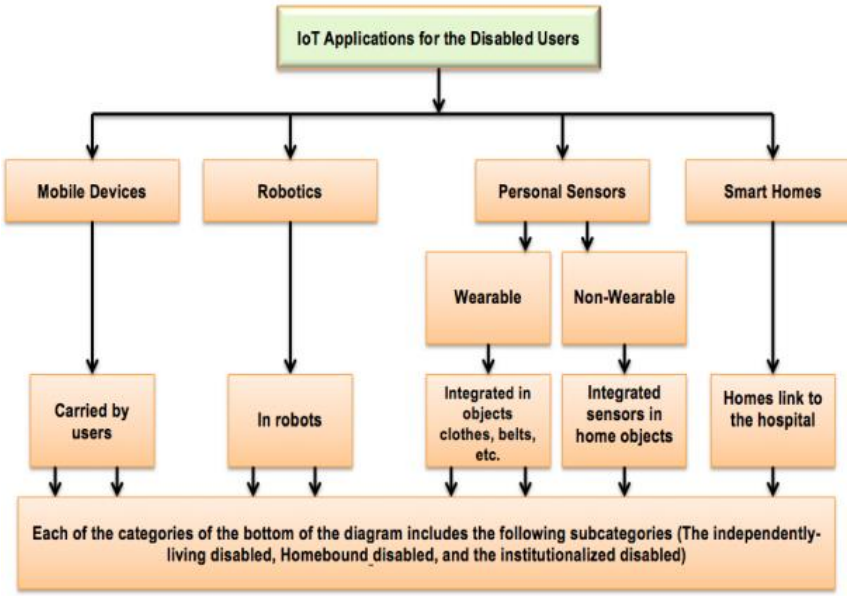

Figure 8: IoT Applications for the Disabled Users (Varghese, 2016)

Figure 8 defines disabled people as independently living disabled, home-bound disabled and institutionalized disabled (disabled people placed inside a facility) and categorizes ways in which IoT is supporting them to enhance their lifestyle.

Fast growing number of the aging population has given rise of more health concerns and healthcare expenses are on rise. In rural areas, healthcare services are not sufficient, as there is a lack of specialized healthcare service. Thus, the disabled have to go for large hospitals and healthcare institutes that are costly. IoT can allow the extension of nominal

healthcare services from healthcare practitioners to the rural region and thus, make health care cost effective for them (G3ict.org, n.d.). These tasks can include maintenance activities like eating, bathing, and dressing, instrumental activities like using electronic items like television, telephone, and dishwasher, and other enhanced activities like learning, socializing, and engaging into hobbies (Coetzee & Olivrin, 2003).

Disabled people can be classified based on their types of disabilities include physically disable and cognitive disability or based on competency including independently lived disabled, homebound disabled, and institutionalized disabled. Physically disabled per would have intellectual or perceptual disabilities that are most common with elderly people of age above 59 as they lack strength and endurance. Cognitive disabilities arise from mental malfunctions causing poor performance in normal functioning. Independently living disabled person could be mobile or immobile. Mobile people can be tracked using GPS and other sensors such as accelerometer proximity sensors, and video camera that can be connected through Bluetooth, Wi-Fi or mobile internet. Homebound disabled people stay at home and need special assistance if they need to get out. Sensor systems can be installed at home for such a person for providing assistance at home with devices such as wearables that can help make their lives easier. Institutionalized disabled need nursing facilities for a long term specialized care (AL-mawee, Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey, 2012).

IoT can help the disabled in various ways such as preventing diseases, preventing disabilities, and managing chronic diseases. Remote monitoring can be done with IoT devices to detect vital signs in patients so that immediate action can be taken by the caregiver to benefit the patient. Three are inexpensive monitoring systems available for capture of such data and complex algorithms can be used on the data that is collected for sending alerts to the healthcare professionals. Early prevention of disease is possible through such monitoring systems as those suffering with some ailment like diabetes can be monitored and thus, prevented from emergencies (CityPulse, 2014).

2.4.3 Patient Health Monitoring System

IoT sensors make a powerful tool for the healthcare sector as it enables remote monitoring of patient's health such that doctors and practitioners can keep track of the health of their patients and give them appropriate advice on the real time to ensure better healthcare (Bachhav, 2018). A remote patient health monitoring system usually consists of a three-tier architecture. The network tier, which is the first tier of the architecture, contains the wearable sensors that act as the sources for data capture and the data that may be captured including latest health condition of the patient like blood pressure and body temperature. The second tier of the IoT architecture includes services that allow the communication and exchange of the data between sensors and other nodes in the network. The top tier of the architecture has nodes used for processing and analysis of the data that is captured for investigation (CityPulse, 2014). This three-tier structure in illustrated in Figure 9 below.

Figure 9: Healthcare monitoring system architecture (Fujitsu, 2016)

Ambient assisted living can be given to the disabled patient so that they are not alone when they face a health problem. Assistance can be provided to such a patient even for the daily routine work through sensing, computing, communication, and intelligence user interface systems connected with the normal objects. Some sensors can also be embedded into a body such as heart beat stimulator or embedded in the furniture at home. These

different types of sensors embedded in different objects are connected such that the data captured is shaped at the same place on the cloud the analysis is provided to the caregiver or the healthcare professional. These devices can also include biometrics that can measure ECG or other alarming systems that allow remote monitoring and care (Fujitsu, 2016).

2.5 Security Concerns

This section addresses one of the 5 research questions identified in Chapter 1 of the research paper i.e.

'What are the security concerns in healthcare IoT systems?'

There are a huge number of devices that are used in IoT networks today and these devices present a variety of e-health scenarios an example of which is the remote monitoring of the patient health (Bachhav, 2018). However, these applications increase the dependence of systems on the technologies for identification of patient and the health condition. This can lead to certain risks for the patients if the data collected is not reliable and the patient information is not authentic. In an open and interconnected environment of IoT systems, the integrity of this data could be at risk as the data while in transit can be exposed to hackers who can make use of the data to take advantage of it and launch attacks against patients including the physical attacks. For example, a thief who comes to know that the person living in a house has a weak heart or a disease like asthma, can use the information and attack on the person's weakness to steal physical stuff from the house(Das, Tuna, Demirel, & Yurdakul, 2017).

Healthcare cyber-attacks can be very dangerous for the patients and could even be life threatening. According to International Standards Organization (ISO); an organization that publishes international standards, healthcare faces large number of data breach incidences and in 2014, the incidences were doubled as compared to the previous year in the UK healthcare system. Healthcare companies have faced 183 data leak incidences and 91 breaches in 2013 while in 2014, there was 44% rise in the data security incidences. Because of such attacks, organizations may have to pay penalties of up to US$1.5 million for a single breach. Further, they need to notify the patients and other affected within 60 days of the

experience of the breach. The breach is also to be reported to media if it is likely to affect more than 500 people as per regulation. In 2015, over 12.3 million Americans were affected by 270 data security breaches in healthcare sector. The healthcare sector lack sufficient resources needed for cybersecurity protection, which is why they are attractive target for cyber criminals (H.Weber, 2010).

There are online applications used for managing healthcare systems that allow sharing of patient information over the web between the hospital and the patient or healthcare professional. This includes the data collected through sensors in the real time and involves tracking of their regular activities (Mohammed et al., 2014). Such applications need to have strong authorization mechanisms. If the authentication mechanism is not strong enough then attackers can exploit the weakness. If a sensor that is connected to, a patient is compromised in this way, it can have dire consequences and can even lead to the loss of life of a patient. Thus, it is very important that these devices are kept safe. IoT sensors used in medical systems for supporting patients continuously keep capturing the data on the hospital visits, patient health stasis, and analyses the same in the real time. These are mostly integrated with a traditional IT infrastructure used in hospital and thus, would have more security challenges. Further, the IoT systems usually are decentralized which makes it even more difficult to anticipate and mitigate security threats and protect humans from malicious intenders (Kahraman, 2010).

Critical infrastructure of hospitals and healthcare systems rely on sensor devices and control systems that are vulnerable to security threats. If these threats are not addressed properly then it can have serious implications on patients. Critical infrastructure of an organization includes the power generation, telecom networks, financial services, and healthcare services. Cyber threats can cause power failure, and malfunctioning of hear care systems causing medical accidents. An attacker if gets access to the patient monitoring system, the attacker would be able to control the medical devices, which can affect the safety of the patient (Zhou, Zhang, & Liu, 2018).

Using cyber security solutions in healthcare IoT is challenging. Latest advances have developed embedded security systems, intrusion detection, and PLC sensor security as some

of the solutions for healthcare IoT protection. However, the fact remains that IoT protocols still lack sufficient features needed for protection of the systems from sophistical cyber threats. GSM being the dominant technology used in IoT networks, the vulnerability is significant. A5/3 or KASUMI algorithm used in IoT has some major weaknesses that can be exploited by attackers. IPv6 protocol that is designed for data-intensive applications is used over low power devices and is vulnerable to DOS attacks. An attacker can send fragmented packets to fake targets through the IoT system thereby blocking services for genuine users in the DOS attack (Kolozali, 2014).

Although IoT protocols are designed with high-end service provision technologies, when the data is encrypted using weaker algorithms, the security level is downgraded thereby giving only the negotiated level of security. Cloud database provides an easy access to storage systems such as NoSQL Mongo databases. A large amount of data that is generated in the real time can be handled by these database systems through a single server. These databases contain sensitive information of patients. If SQL injection attacks happen on such databases, the impact could be devastating for whole database and even the cloud based content management system (Kolozali, 2014).

Medical professionals can use online systems for accessing patient records as well as sharing them with other professionals. The data that is shared in this way can be very sensitive and confidential. A breach of this data could have negative impacts on both the patient and the medical institution. If the healthcare system has to be protected from such threats, it is essential have advances algorithms used for accounting and authorization. Hospitals also need to follow certain legal procedures such as those defined in Health Insurance Portability and Accountability Act (HIPPAA) as these can help in handling patient information that is accessed over the cloud (Nath & Som2, 2017).

2.5.1 Security Solutions

The security of IoT-based healthcare devices is extremely crucial as single breach or malfunction can cost someone their life. There are varieties of security solutions that are used for the protection of IoT based healthcare systems. The design and implementation of most

security systems is difficult and challenging due to their low computational resources. However, all these solution systems must have some key features in common. Firstly, as far as physical space is concerned the solution must be small and accommodating. This is because most IoT-based healthcare devices lack the capacity for large drivers. Therefore the solution is expected to be lightweight in terms of both the device they are intended to run on and the codebase implemented. Moreover, it should have high processing power so it can work efficiently and effectively even on a low power device (Sandoval, 2017).

Use of authentication for data access through healthcare portals on smartphones is one common method of providing security. The authentication is cryptography based such that the data is encrypted and can only be decrypted with proper authentication. Authentication can provide security by preventing unauthentic users like hackers from logging into the system. However, the systems being complex with involvement of IoT devices and internet-based applications, high-end security solutions are needed and just basic authentication may not be sufficient as a security provision (Pathak, 2017).

With increasing connectivity and trillions of user objects joining the network the number of unique authentication keys required is increasing. Most developers are using RFIP-technology as it consumes less resources and is also less costly. In fact, Aggarwal and Das (2012) created one such lightweight protocol to integrate with the existing security system that also maintained the system's efficiency. Continuing their work Torjusen et al., (2007) introduced run-time verification enablers in a security system known as ASSET. These developers also introduced features like dynamic context monitoring and adaption.

Secure initialization protocols have also enabled IoT based healthcare devices to be additionally secure. One such technique was developed by Hou, Li and Guttman (2013) by the name of Chorus for secure initialization of a group of wireless devices. This two layer protocol protected the devices from external cyberattacks by the use of in-band group message authentication and group authenticated key agreement. The system also had additional features of scalability due to its low hardware and computational requirements.

Another way of making healthcare-related IoT devices secure is to create a separate network, one that allows centralized monitoring of the devices through aggregated hubs. It is

imperative that the kind of data the devices interact with is also strictly monitored. This eliminates the chances of hackers to penetrate the network.

2.6 Addressing Privacy Issues

Privacy issues may arise, as many data that is private to a patient gets stored in the database that is filled by the data captured using IoT devices. A patient health record is maintained in databases that has to be kept confidential for which an ABE technique can be used which involves encryption of the data through the use of algorithms like MD5 and AES before it gets stored in the database. A healthcare system works in two security domains including public domain and personal domain such that the two domains may have different security requirements. Public domains could have users like doctors, nurses, and medical practitioners or researchers while the personal domain would have the patients. A privacy measurement scheme can be used for detecting if the content collected from the sensors is sensitive and if it should be kept in the public or private domain according to which access rights may be provided to respective roles in respective domains on the collected data (Raggett, 2016).

Privacy attacks can also include false injection of data that can cause damage to a healthcare or IoT application. It is difficult to counter such an attack in IoT as the devices have constraints in the use of resources such that standard security solutions cannot be implemented inside them. To overcome these challenge, a distributed cyber-attack detection system is needed (Raggett, 2016).

Data eavesdropping and maintaining confidentiality over the wireless can be taken care of by using rolling-code cryptographic protocols or through a body-coupled communication. A bi-polar data hiding technique can be used for protection of images, which would allow the doctors to add a digital seal to the image within a patient health record document. Public Key Encryption can help improve the data confidentiality through and effective data encryption mechanism (Sajid, Abbas, & Saleem, 2016). Moreover, IEEE standard 802.15.4 provides guidelines to protect different access layers of an IoT architecture

and can be used as a tool to add safety features to a system (SathishKumar and R. Patel, 2014).

2.6.1 Addressing Security Issues for Physical Objects

The physical objects like sensors can also face security issues as they have constrained resources and cannot run complex security algorithms. More of traditional architectures may be used wither these objects and thus, unauthorized access may become easier for the attackers. An IoT system has four key components that include a person, intelligent object, the process and the technology ecosystem. All these components interact with each other and thus, affect the security factors like identification, privacy reliability, safety, trust, and responsibility. Physical devices such as RFID tags that also have such different interacting components can face a variety of security attacks such as denial of service, cloning, spoofing, service denegation, and in the middle attack, abuse, and so on. Certain security defense techniques can help protecting RFID tags such as system chaining for avoiding unauthorized reader, encryption through AES or MD5 algorithm, and so on. These solutions help main security, privacy and integrity of the healthcare system for its users (Shoham, Harris, Mundt, & McGaghie, 2016).

2.6.2 Security Issues for Communication Technologies

Communication technologies can face security issues such as DOS attacks, flooding, black hole attack and homing attacks. These technologies are very prone to security pairing and can be exploited by attacks through tracking, data theft, spanning, man in the middle attacks, and malicious code injection. Intrusion detection techniques can be used for securing communication systems as they can detect malicious activities, provide a firewall and anti-jamming capabilities. Encryption can be used for maintaining confidentiality of the data that is transferred over the wireless network. Some encryption algorithms that can be used for this include DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard). LTE devices are secured through techniques like Sequence

Number synchronization (SQN) and Re-authentication protocol (Extensible Authentication Protocol Authentication and Key Agreement) (Wind, 2015).

2.6.3 Security Issues for Applications

Security issues can also occur in applications that are used over cloud for the IoT network management. To ensure that security of the applications is maintained, a common measure that has to be taken is securing of the data access points. This can be done with protection mechanisms at the points where patient health records are shared over the cloud. At this point, a malicious attacked can get to the stored medical data and can modify the same to affect the patient. Thus, it is essential to keep the access points most secure in the system. Some of the methods that are used in the healthcare IoT systems for such protection include use of security algorithms like Ciphertext-Policy Attribute-Based Encryption (CPABE), which uses Attribute-Based Encryption (ABE), works on the Elliptc Curve Cryptography (ECC), and uses Bilinear Mapping (Zhou & Lutfiyya, 2016).

2.6.4 Security Issues for Personal Protection

Data protection and the privacy of the individuals are the two interconnected concerns in the information security. IoT networks involve capture and transfer of a large amount of data that can include personal and confidential information. IoT devices can also be upgraded beyond the simple data capture such that new possibilities emerge. These new possibilities also raise new risks in the security of the individuals. The IoT sensors can collect a large amount of data on physiology and environment of a user through smart devices such as a laptop, smart phones and digital wearables. These smart things when upgraded can be controlled such that the physical actions are influenced. Communication can occur between objects that are connected in the IoT network automatically so that they exchange the data with each other and act upon the same (Zhou & Lutfiyya, 2016). This automatic interaction and action can affect the privacy, confidentiality and integrity of the information that is being exchanged. The personal information that IoT devices contain may not just have the data of the person using the device but also of other people who may be connected to the user or

related to him or her in some way. The data can contain the details of one's social identities such as name, address, mobile number, and more. IoT devices contain a lot of data but are not advanced enough to implement all layers of security that can protect this personal data which may require taking care of a variety of privacy policies that could be situational or context driven. More personal data collection can raise issues of unlawful processing, profiling, tracing, purposing, mission keeping, and many more problems. Law enforcement in this context needs understanding of the protection rights of users, principles of the field of data, ownership of data, control procedures, privacy violation, and IoT environment characteristics. There can be concerns of identity theft with the data made available through IoT networks openly. For instance, contactless credit cards can be read without any need for the authentication which can give an opportunity to the hackers or attackers to possess the identity of the users in the bank account (Wind, 2015).

Malicious attacks on IoT devices can result into a compromise of the device and the control goes into the hands of the attacker through which unauthorized access to the personal data is gained which increases the risk for the users. More often users are restricted to a specific service provider and cannot freely move to another which puts limitations that can be detrimental to the security. In the healthcare sector, this can have significant security and privacy risks by putting integrity of a patient data at risk. A health application can expose the data on the disease a person has to attacker which can be used for launching a physical assault thereby causing personal risks to the health and life of the patient. As IoT systems automate the decision making process, the control over the data and decisions that trigger specific actions from the devices is lost. This is a concern for most people and thus, there are several data protection laws practiced globally to protect data used this way (The Economist Intelligence Unit Limited, 2018).

2.7 Security Standards

2.7.1 ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)

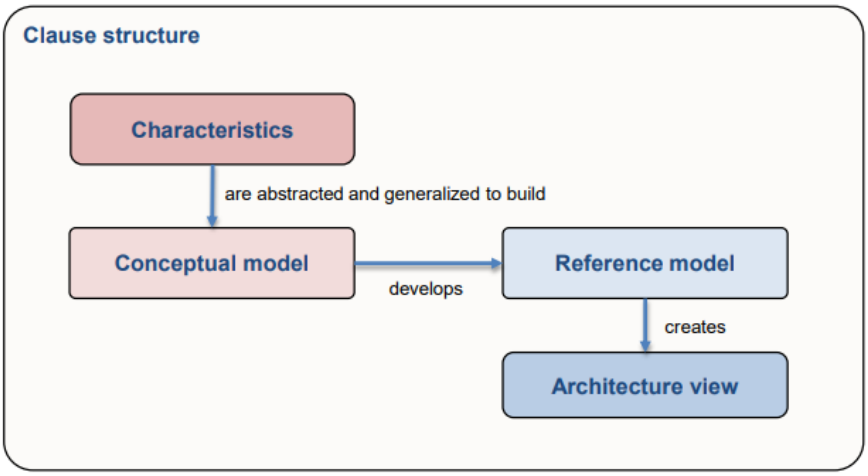

Figure 10: IoT RA (Islami, Daehan, Kabir, Hossain, & Kwak, 2015)

ISO/IEC 30141 defines the IoT architecture including the characteristics of the devices as explained below (Islami, Daehan, Kabir, Hossain, Kwak, 2015):

System characteristics: System characteristics include configuration, subscription to real-time services, self-description, network management, communication management, operations, and distributed systems. Real time services refer to a mode of operation which involves computation based on a real time data such that the results can be used for monitoring or controlling processes or devices. IoT systems are required to operate in the environment where data keeps flowing continuously such that responses needed to the events emerging has to be in the real time. This would require real time streaming of the process and immediate action on any event as soon as the data is received to ensure that an appropriate action is taken on time (Mishra & Pandey, 2013).

Service characteristics: Most times, the IoT services are managed by the providers and used by organizations by taking a subscription which allows registration of specific IoT users. The process of subscription needs to have clarity on the re-requisites needed and the payment to be paid against subscription for the arrangement to work. A service that is subscribed to

would involve installation of IoT devices and configuration of the software in them. With the subscription model, the company ca save itself from the need of purchasing own equipment's and working software as well as taking care of operations and maintenance. Specific characteristics of these services can be context awareness, content awareness and timeline (Bourouis, Feham, & Bouchachia, 2012)

Component Characteristics: These include composability, share ability, connectivity, identification, modularity, and discoverability.

Compatibility: Well defines components should be provided with the legacy support.

Usability: These include manageability and flexibility

Robustness: These include availability, safety, integrity, and confidentiality

Other characteristics include data volume, variability, velocity, variety, veracity, heterogeneity, scalability, trustworthiness, and regulatory compliance (ISO, 2018).

As the number of connected devices increases to reach billions, solving interoperability issues has become imperative and that is why we need IoT standardization. It is important because it can bridge the gap between protocols and reduce the overall cost of manufacturing and transporting components (Internet of Things (IoT), (2017).

2.7.2 ISO/IEC AWI 21823-1: Interoperability for Internet of things systems (IoT)-Part 1

This model of IoT identifies a variety of IoT components that work synchronously to generate desired outcomes of the network technology. These components include the heterogeneous devices that could be connected to each other. Communication can happen between them for which the best communication network or mode is chosen on the basis of its availability, latency, bandwidth, and jitter (ISO, 2014).

This standard is used for IoT and related technologies like sensors and big data to provide interoperability since many stakeholders and technologies are involved in a wide range of applications. There are 50 experts of the field who examine the data standards used across the world and identify specific requirements of the market where the system is needed

to be implemented so that they can be incorporated with the standards. This architecture gives the framework for understanding interoperability in IoT (Garg, 2017).

2.8 Summary of Literature Review

A thorough analysis of the literature review reveals vital information about IoT, its architecture, components, applications, contribution to healthcare and relevant security concerns in mobile applications, communication networks and patient information databases. It gives the reader a deep insight of the current prevalent security issues and how they can be adequately addressed. This chapter acts as a foreword to the following chapters in which specific security systems are investigated and their key features explained.

Chapter 3. Methodology

This chapter explains the research methodology including the tools and techniques that were used for the data collection and analysis. It presents the research design and justifies the choice that is made. The chapter covers the ethical aspects and the limitations of the research methods. It serves as a plan for conducting the research on innovative IoT healthcare systems and technologies.

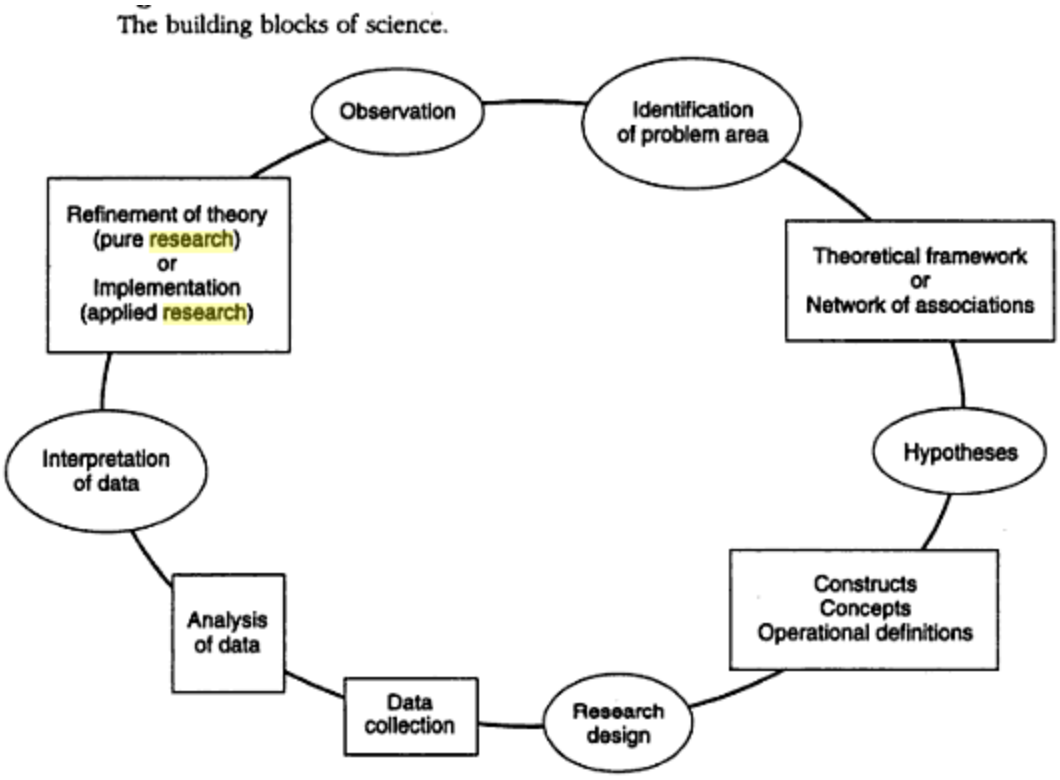

Figure 11: Scientific research design (Stanley and Wise, 2002)

Figure 11 shows how a research designing process is shaped. It involves identification of problem area which is explored through the use of theoretical framework that gives the base to the problem such that a hypotheses can be formed to help a researcher build the investigation upon it. Hypothesis constructs can create a research design which would give the researcher a guidance on how to collect, analyze, and interpret data. Once the

data is interpreted, the original problem that was observed could be revisited and the related theory can be refined based on the new findings. As suggested by the model, a scientific research is a process of systematic investigation of an existing area of knowledge and the refinement of related theories using the empirical evidence (Us.sagepub.com, n.d.).

3.1 Research Philosophies

It is not always possible to choose a single philosophy for conducting research as research needs to explore the realities that may not be understood by a single approach and may take on a combination of a few (Stanley & Wise, 2002).

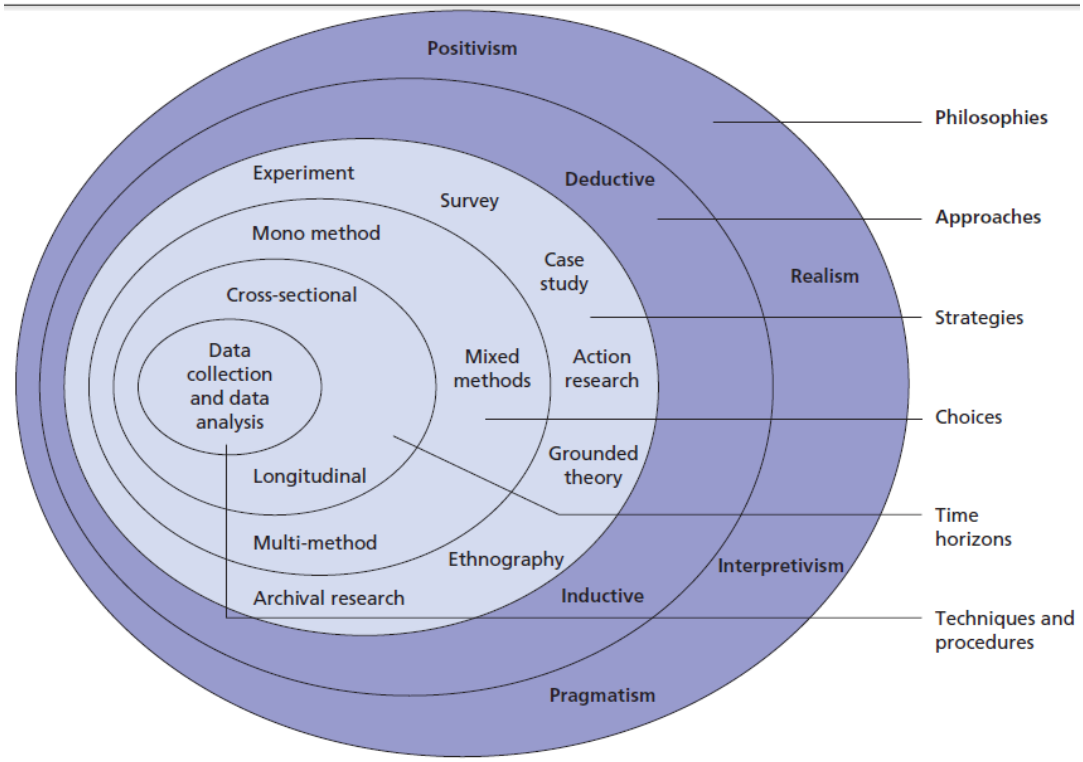

Figure 12: The research onion (Davidavičienė, 2018)

The research onion (Figure 12) can be used for understanding the interconnections that exist between different philosophies and their applications. Its greatest quality is its versatility which allows it to be applied to a large variety of different researches (Saunders et al., 2007).Key philosophies that exist in the first layer of the research onion include realism, positivism, interpretevism and pragmatism. The researcher can make a choice from these

based on his own understanding of the knowledge and on the basis of the need of the research subject, as long as it adequately answers key questions and fulfills the objectives of the research. A positivist view says that there exists reality that has to be empirically tested through the use of scientific investigative methods and thus, may suggest the use of data collection and analysis of the same using statistical or analytical tools (Snieder & Larner, 2013).

Interpretivists believe the opposite and say that there can exist several versions of reality such that it can only be understood by exploring the perceptions from different angles. Such a theorist would seek the truth from different philosophical lenses for understanding. Pragmatists do not trust a single method and thus, suggest inclusion of both empirical and interpretivist approaches to discovery to be used so that they can be tested to verify the findings of each other (Beiske, 2007).

3.2 Research Approach

The question that this research addresses is if guidelines for the protection of personal information used in health IoT devices can be developed? As the topic is driven by technology and its usage, the researcher believes that there exists a reality in the threats that IoT systems face and of the methods that can be used to mitigate them. Thus, the researcher chose the positivist view of research considering the existence of a reality that can be tested or explored. The researcher collected data from previous researches that have already explored different healthcare systems, architectures, and innovation in the field and evaluated their level of consistency in safeguarding sensitive healthcare related information of patients.

Considering the epistemology, in this research, authoritative knowledge was used that already existed in the research field of IoT and thus, involved the review of the professional literature on the subject. Thus, the research explored various healthcare systems and architectures used in IoT systems to determine how they ensure reliability and security of data that is used or exchanged in the system.

The research studied the previous literature on the themes of IoT based healthcare systems, secure IoT architectures, data reliability, and data security in IoT. For this, the data was

collected from previous research reports, books, and journals and the resulting literature was critically analyzed by the researcher to assess the defined methods so that those giving high levels of reliability and security for IoT data can be recommended (Denzin & Lincoln, 2000). This research was conducted using a positivistic research approach in which the previous qualitative data was logically gathered and critically analyzed, since its purpose was to understand the protection of personal information in IoT based healthcare systems that already exist and not to develop a new healthcare security system or investigate the feasibility of pioneering one.

The positivistic research approach that the author adopted adequately answered the research question due to several reasons. Firstly, such an approach extracted from the research onion established and acknowledged a reality that is that IoT based healthcare systems exist and explored their current effectiveness, benefits, shortcomings, limitations and future prospects which is the main topic of focus. Secondly, the tests were based on data collected from various researches. These findings in collaboration with the critical analysis of the researcher gave a comprehensive view of the problem at hand and if and how this can be addressed.

3.3 Research Process

As mentioned in the previous section, the author adopted a positivistic approach of research to recollect and analyze information from a variety of sources. Such a method is normally deductive instead of inductive and the role of the researcher is limited to data collection and interpretation in an objective manner (Research-Methodology, n.d.).Figure 13 below shows the difference between a deductive and inductive approach of research, identifying similar processes with only a reversal in order.

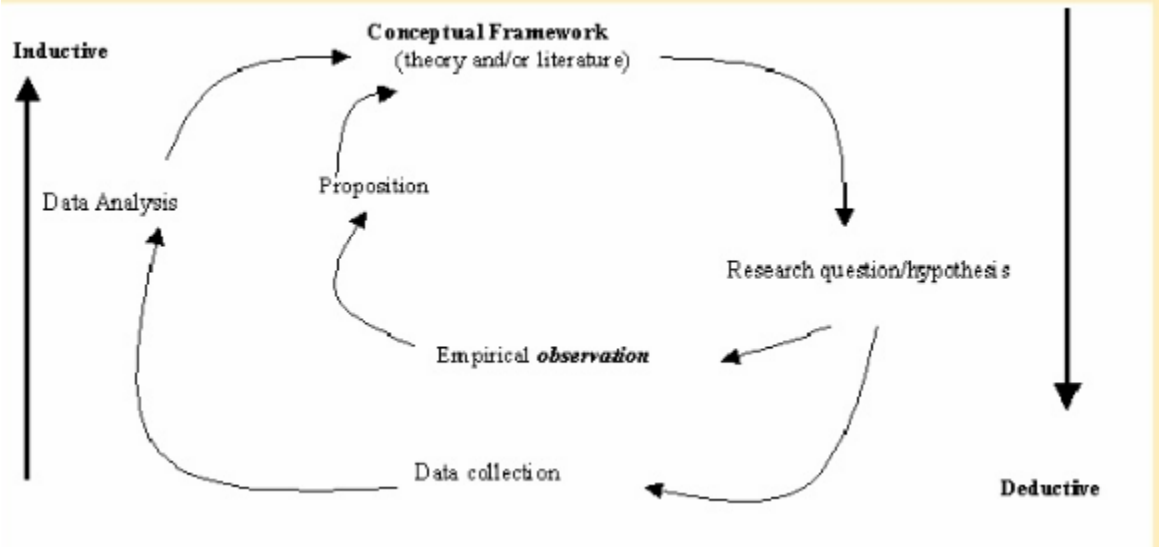

Figure 13: Inductive and Deductive Research Approach (Rudestam and Newton, n.d.)

3.4 Data Collection and Analysis

This study made use of the secondary qualitative data that was collected from sources including books, articles from journals (peer-reviewed, refereed and published), research reports from researchers, company reports, news articles, and research websites, therefore, their authenticity was not be questionable.

In order to filter and critically analyze information that was relevant to the topic of the thesis and adequately answered the research questions the following steps were involved. I have used the library databases and Google as a start to look at contemporary material. The first step was to collect these sources of information and this was mostly done over the web. Some common search phrases included 'IoT in healthcare', 'IoT based healthcare systems,' 'IoT based healthcare devices,' 'Privacy risks in healthcare systems,' 'Protection of information in IoT-based healthcare devices,' 'Security risks in IoT,' etcetera. The next step was to determine the reliability of the source. For example in case of journal articles peer-reviewed and refereed articles were preferred and in case of conference proceedings, a high citation index and international recognition were factors that were considered. Sources that

were older than eight to ten years were eliminated. Each piece of information was thoroughly read, important points noted down, accompanied with a constant search to understand difficult terms and descriptions. The next step was to critically analyze the data to determine its relevance. This was done by establishing the relationship between the thesis objectives and the short-listed points in order to evaluate how well the latter answered the research question. The most critically relevant information was documented including important deductions made based on it.

3.5 Sources of Data

3.5.1 Maintenance of authenticity

In research processes based primarily on data collected from various sources the maintenance of authenticity can be extremely crucial. As mentioned in section 3.4, the different sources that were employed included journal articles, conference proceedings, research papers, electronic databases, company websites etcetera. In order to ensure authenticity for instance journal articles that had high impact factors, were published in internationally renowned journals and were either refereed or peer-reviewed were chosen. Likewise, websites of internationally acclaimed universities, academic societies or industrial companies were accessed for additional information. Approximately fifty different sources of information were reviewed (out of which roughly thirty of them were relevant research papers) and useful information was extracted from them. Some of these sources are discussed in the following sections.

3.5.2 Journals

Journal articles were largely accessed online from eminent websites like *Google Scholar, ResearchGate, Semantic Scholar* etcetera. Some of the journals reviewed are listed below:

- International Journal on Recent and Innovation Trends in Computing and Communication
- International Journal of Computer Science and Mobile Computing
- International Journal of Advances in Electronics and Computer Science
- International Journal of Engineering Sciences and Research Technology
- International Journal of Research in Computer Science Engineering and Technology
- Asian Journal of Applied Science and Technology
- IEEE sensors journal

3.5.3 Conference Proceedings

Research papers, abstracts, extended abstracts, presentations, manuscripts and other technical documentation presented at international conferences were also viewed as reliable sources of valuable information. In order to avoid outdated and archaic data the timeframe for these proceedings was set to eight years. Material older than this and outside this time frame was discarded. Some important conferences whose proceedings were critically reviewed are as follows:

- Annual IEEE Consumer Communications and Network Conference
- Project Management Practitioners Conference
- International Conference on Software Engineering
- IEEE Symposium of Security and Privacy
- Information Systems Audit and Control Association

3.5.4 Online Databases

In order to avoid any unfortunate encounter with unauthentic data website search was restricted to scholastic databases, company profiles and reports and reliable encyclopedias. Some of these include:

- Computer Science, Harvard University
- Middlesex University, London

- University of Duhok
- Cisco Systems, a multinational networking hardware company headquartered in Silicon Valley
- VMware, a computer software subsidiary of Dell Technologies

3.6 Limitations

As this study only made use of secondary literature for understanding the concepts of security and reliability of IoT systems in healthcare, the research may not be able to explore the real experiences of people who may have faced security threats in healthcare. The perspectives that were explored in this research were largely of the researchers who had conducted the researches in the past and do not have the critical view of the healthcare professionals that may be needed. However, despite these limitations, the research findings can still help in collaborating information studies by different researchers to get a comprehensive view which would be supported by the critical view of the researcher.

3.7 Ethical Codes

As per Cooper & Schindler (2006), a good research always considered the ethical codes and followed them to ensure that the research activities are not harmful to any person, community or industry. Thus, in this research also, the researcher has taken care of the ethical codes including maintaining of authenticity of data by only taking the inputs to research analysis from authentic research. Further, to maintain integrity of the data and the research finding, the researcher has ensured to not have a biased view on the research subject but only explore it critically and logically to deliver object insights.

Chapter 4. Results

This chapter discusses and analyzes the data extracted from various sources including books, articles from journals, research reports, company reports, news articles, and research websites. The research process compromised majorly of searches made online under the keywords of 'IoT in healthcare' and 'IoT based healthcare systems,' and others and reviewing articles that contained these keywords. The library search for more information comprised of narrowing it down to the IT genre. Much of the information about the security systems chosen was taken online from university portals like Harvard University and Imperial College, journals like the International Journal of Computer Science and Mobile Computing, conference proceedings like SenSys 2nd International Conference on Embedded Networked Sensor Systems and other sources of scholarly articles and books online. In order to understand how the results were compiled it is important to review the processes that led to them. This is discussed pictorially in the next section.

4.1 Research Process Diagram

Figure 14 given below shows the process diagram for a pictorial representation of the steps, employed in the research of security systems for IoT in healthcare. It presents a systematic order of all the steps discussed earlier in this chapter from the point of identifying the problem to the final results and conclusion.

The research process commenced with the identification of the problem that was to determine how protection of personal information was made possible by IoT used in healthcare. The second step was to review literature relevant to this topic. This included identifying various security concerns surrounding IoT in healthcare, categorizing them as issues related to physical objects, communication networks, applications and storage databases, and determining methods by which these issues can be resolved. Besides that, for a more holistic understanding of the reader, IoT architecture, components and its involvement in healthcare was also discussed. The next step was to give more clarity to the research problem. At this point the author streamlined his research to focus on specific

security systems, their key features, and capabilities and how they made protection of personal information possible. Once the research problem was narrowed down to a more specific goal, the author devised an instrumentation plan. .According to this roadmap, the author collect information from different sources including journals, books, magazines, websites and university portals, the authenticity of which was determined first, selected security systems and then conducted a thorough research on each to adequately answer the research question. Data analysis included selecting those systems that offered a high degree of protection and were extracted from authentic sources like published books and magazines, peer-reviewed journals etc. Conclusions were drawn on the basis of the analysis performed.

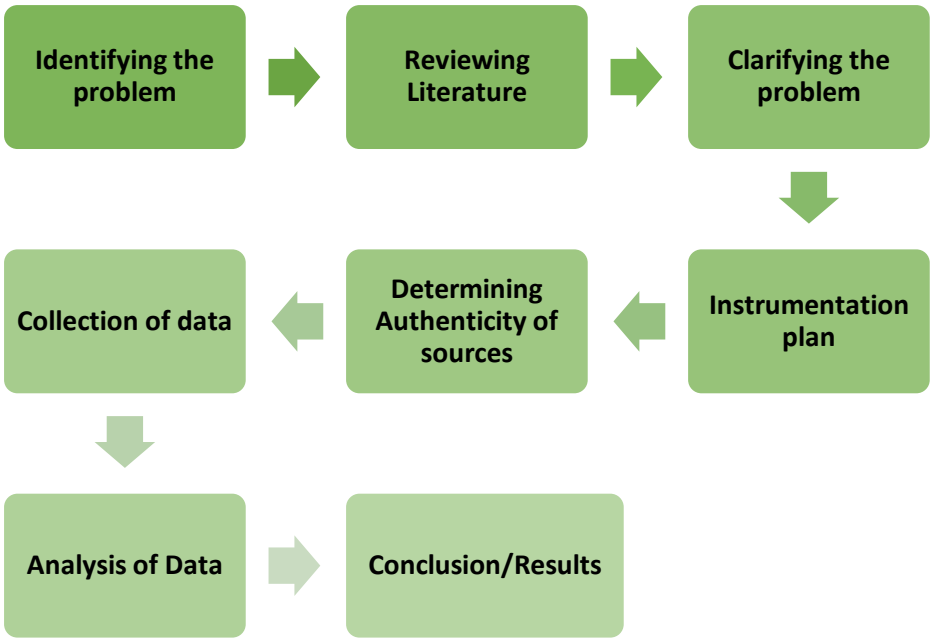

Figure 14: Research Process Diagram (Human Kinetics Europe, n.d.)

The table given below summarizes all the sections of the chapter including IoT based healthcare systems like CodeBlue (Shnayder et al., n.d.) that revealed Elliptical Curve Cryptography (ECC) (MS., n.d.) for encryption and TinySec(Karlof, Sastry and Wagner, 2004) for key generation, Body Sensor Network (Espina et al., 2014), Secure and Efficient

Authentication and Authorization (SEA) Architecture like Datagram Transport Layer Security (IoT ONE., n.d.), including FDA guidelines on security and usage of medical devices. These systems were chosen due to their technical complexity, sophistication, accuracy and reliability.

DATA	DESCRIPTION
1. IoT Based HealthCare Security	
1.1 CodeBlue	A software based medical sensors network that collects health related data to monitor patients and answer questions in real-time. Led to the discovery of TinySec, ECC and DTLS.
1.1.1 Elliptical Curve Cryptography (ECC)	An encryption technique based on elliptical curve theory. Compared to RSA it is faster and requires less storage.
1.1.2 TinySec	A link layer security architecture for wireless sensor networks. Offers the three basic security protocols; message integrity, confidentiality and controlled accessibility. Uses initialization vectors, cipher block chaining and MAC codes.
2. SEA Architecture	AN IoT based medical security architecture consisting of a medical sensor network (MSN), smart gateways, a secure back end system and online clients.
2.1 Datagram Transport Layer Security	A protocol capable of securing blocks of data of varying sizes known as datagrams.
3. FDA guidelines	A descriptive analysis of guidelines issued by the FDA for development of medical communication networks, designing safety protocols and other relevant security measures.
4. Body Sensor Network	A BSN architecture based IoT health-care system that checks workflow compliance across five key components including data, activities, location, time limits, and resources. Has basic modules like login, registration, key authority control, LPU, and BSN care server.

CISCO Healthcare Network	This kind of solution is directed towards providing a unique experience to the patients along with maintaining his records in a careful manner. The innovative onsite and mobile technologies helps the patients to obtain personalized treatment along with maintaining records of the patient in a safe manner.

	Proper and detailed guidance to the patients is also provided to the patients so that they are able to use this system in an effective manner.

Table 1: List of security systems

Table 1 in fact answers an important concern that was raised in section 1.1 i.e.

'What architecture can be used to secure healthcare IoT systems?'

One can tell after reviewing the table that the security of IoT based healthcare can be ensured by numerous different architectures and protocols, some of which are discussed in this research paper.

4.2 Product Solutions

4.2.1 IoT Based healthcare security

A popular healthcare project called CodeBlue was launched by Harvard University in which wireless medical sensors were used for monitoring patients. The project revealed that there is a deep need for securing IoT systems used in this way for patient care through key generation and data encryption. CodeBlue provides protocols and services for node naming, discovery, any-to-any ad hoc routing, authentication, and encryption (Malan et al., 2004).CodeBlue prevents network congestion and information overload by using filtration and aggregation, giving physicians the flexibility to choose the amount of information he/she receives from each patient (Malan et al., 2004). Data collected from different wireless sensors can be rallied to fixed terminals and then integrated with existing patient records in the hospital's database. Multiple concurrent queries can be issued by physicians using CodeBlue (Shnayder et al., n.d.). It can also be engaged in ad hoc fashion in case of an emergency situation. Under ad hoc conditions the communication network does not remain fixed, in fact when powered on allows devices to rapidly join the network, even those from other medical facilities (Shnayder et al., n.d.). Faulty linkages can be instantly detected and re-routed. The network also supports dynamically transforming classes of sensors and user devices.

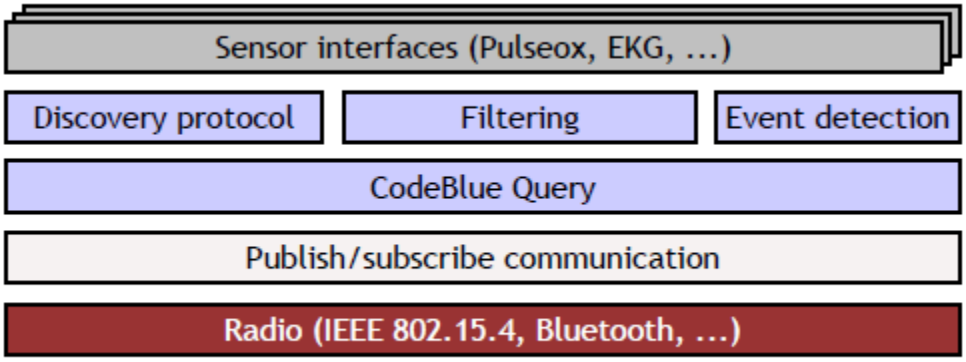

Figure 15: The CodeBlue software architecture (Shnayder et al., n.d.)

Figure 15 shows the software architecture of a CodeBlue prototype developed at Harvard University. The sensing interface is based on multiple wireless sensors including pulse oximeter, EKG, motion capture and electromyography. Discovery protocol provides users with a means to know which sensor is participating in a network so they can subscribe to a network of their own choice. The CodeBlue Query interface allows users to receive periodic and triggered patient status details (Shnayder et al., n.d.). Moreover, CodeBlue is based on a publish/subscribe communication model. In a hospital's sensor network there are many different types of sensors that not each individual is concerned with. In such a communication model data from sensors are relayed to specific channels that any user can subscribe to according to his/her needs or interests.

During the development of the CodeBlue prototype a few methods were discovered that could help in securing the devices used on patients for their monitoring and these included Elliptic Curve Cryptography (ECC) for encryption and TinySec for key generation. Protocols can be used for security such as Datagram Transport Layer Security (DTLS).

Efforts have also been taken for securing gateway for applications and architectures in the eHealth care services. Smart 6LoWPAN border router can be used for taking decisions to ensure reliability of data and securing the outcome using a Hidden Markov Model (Shen et al., 2011). UT-GATE is a smart healthcare gateway system that can be used for building intelligence in to the IoT based healthcare system (Rahmani et al., 2015). These gateways

can be used for storing and processing data locally so that the preliminary search results can be provided instantly through data aggregation. This reduces the need for connecting to a remote server every time a search is requested.

4.2.2 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public-key cryptography which is based on an asymmetric algebraic structure (Stolbikova, 2016). ECC needs smaller keys as compared to other cryptography algorithms like RSA and still can provide similar level of security. This reduces the transmission and storage needs of algorithm. ECC is recommended by National Institute of Standards and Technology (NIST) for key exchanges and digital signatures. NSA also uses ECC algorithm for protecting their top secrets that has replaced the earlier 384-bit ECC keys. ECC as an algorithm is quite complex and a wrong implementation can be disastrous. Branching errors, cache-timing errors and leakage of private keys are some of the possible calamities. However, overall ECC implemented correctly provides a high degree of security. This also answers one of the research questions that with the right IoT architecture, healthcare systems can be made more secure. Figure 16 below gives some eminent advantages of implementing Elliptical Curve Cryptography.

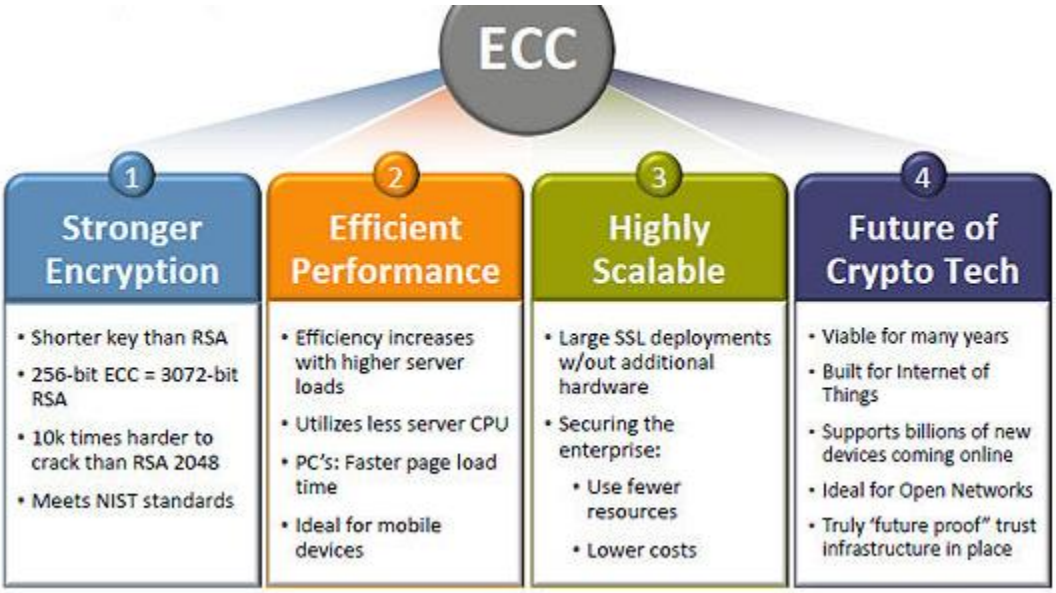

Figure 16: Advantages of ECC (Shimel, 2013)

4.2.3 TinySec

TinySec is a layered security architecture that is used for wireless sensor networks so that data can be communicated securely over these networks. It provides the base for the implementation of a high level security. The system is a software based on a minimum Mica 2 hardware that consists of 8 MHz 8-bit Atmel CPU, 128 kb of the instruction memory, 4GB RAM, 512 kb flash memory, and 19.2 kbps radio. TinySec guarantees the confidentiality, integrity, and authenticity of the messages being sent over the network. However, it does not protect the system from resource consumption attacks, physical tampering, and node capture attacks. The link layer security provided by TinySec ensures that each data packet that is transmitted over the IoT network is encoded and decoded for protection. Linked architecture can immediately detect bad packets from the data that is transmitted by multiple sensors for the base station. With this detection, the resources are saved. There are some design goals of security that TinySec can help achieve in a healthcare system. These include:

Access Control: The architecture ensures that unauthorized parties are unable to participate in the message exchanges through the use of MAC coding.

Message Integrity: If any message that is transmitted is modified in transit then it can be detected using the MAC code immediately in the TinySec architecture.

Message Confidentiality: The architecture makes use of encryption to keep the information needs of patients in the system private from the unauthorized users.

Replay Protection: A legitimate packet, that is sent earlier, can be sent again by the unauthorized user for overhearing it. Overhearing can be detected by the algorithm as it increases the message length resulting into decrease in throughput, increase in latency, and increase in power consumption. A typical defense to such an attempt is the use of an associate counter that is attached with each message that is sent but it would still need higher level protocols to deal with such situations.

Ease of use: For providing ease of use, the system provides transparency and portability. With support for different hardware including radio and CPU and any porting, portability is achieved.

MAC code which is the primitive for the security as defined earlier is a solution for maintaining integrity and authenticity of messages. It uses CRC cryptography for security. A private key is shared between the sender and the receiver. The packet that is sent contains a MAC code which is computed by the sensor using a private key. This MAC code is also computed at the receiver end and if the two codes do not match, the receipt of the message is rejected (Patel, Singh, & Pandya, 2017).

Initialization vector is another security primitive that is used in the TinySec which provides an encryption mechanism. The vector algorithm helps in achieving semantic security, adds variation to the encryption, tradeoffs the message length between overheads and the resource usage. TinySec can be used either only for authentication as in TinySec Auth or for both authentication and encryption as in TinySec AE. TinyAuth ensures that the source from which the data is received are authentic and is often used for public data encryption. TinySec AE not just ensures that the source is reliable but also prevents unauthentic users from seeing the data using MAC coding (Lake, Milito, Morrow, & Vargheese, 2013). A comparative study of different architectures has revealed that the total size and packet overhead of TinySec-Auth is the least, followed by TinySec-AE, while the opposite is true for transmission time (Figure 17).

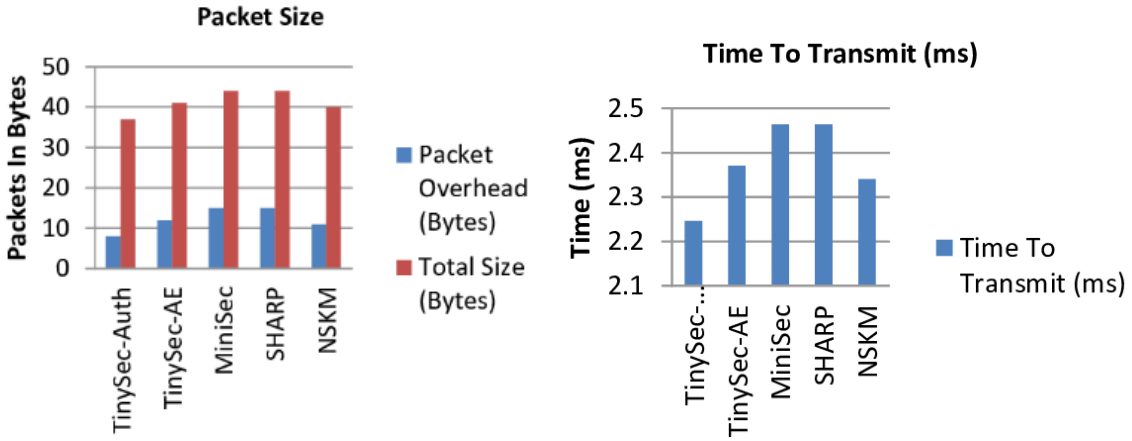

Figure 17: Performance Comparison of different key management schemes (Gawdan and Sarhan, 2016)

TinySec uses Cipher Block Chaining as the encryption algorithm and IV message format that minimizes overheads. Ciphers used in this method can be stream ciphers or block ciphers. Steam ciphers are faster than block ciphers but they have limitations to vary messages and thus, block ciphers are preferred such as DES, RC5 and AES (Karlof, Sastry, Wagner, & Ruggieri, 2017).

4.2.4 Secure and Efficient Authentication and Authorization (SEA) Architecture

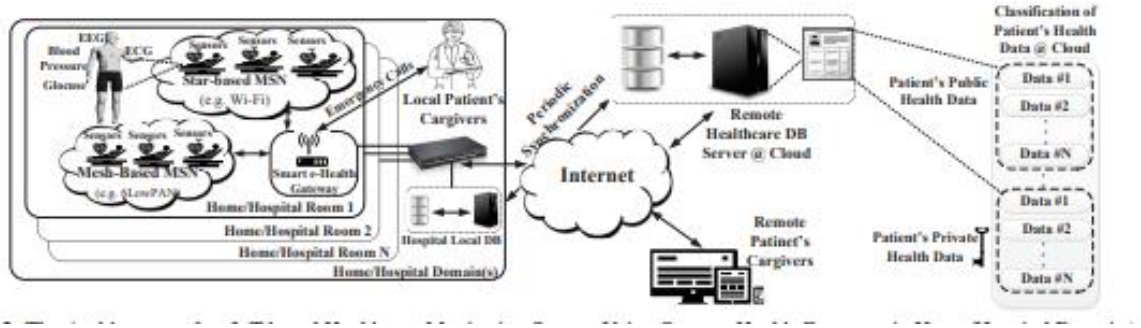

Figure 18: SEA Architecture (Begum & Venugopal, Comparison of various Techniques in IoT for Healthcare System, 2016)

Figure 18 shows the IoT based healthcare system used for monitoring patient health and providing connection between the hospital and the patient connected sensing devices through the use of a smart e-health gateway. Sensors are implanted to the wearables that patients carry. These sensors record the health information of the patient. The health information is supported by additional general information about the patient for identification of various patterns of situation such as location, temperature, date and time. The architecture had three key components that include medical sensor network (MSN), smart e-health gateway, a secure back end system and web clients (Begum & Parveen, 2016).

Medical sensor network involves sensing, identification, communication, bio-medical and contextual signals. These signals are captured through the IoT devices connected to the patients for monitoring their health situation and equipment used for diagnosis or treatment of patients. These signals are transferred through the secure gateway using secure protocols like SPI, Bluetooth or IEEE 802.15.4. The gateway serves as a touch point between the MSN and the internet or local Ethernet and supports various communication protocols. Data is received from the MSN or different such networks, protocols are converted, and other services are provided such as data aggregation, filtering, and reduction of dimensionality. Remaining components of the system are in the back end system. They include local switch, data warehouse, local hospital databases, and data analytics servers (G & A, 2016).

Local databases that are used in the hospitals are synchronized over time with the latest patient data that is generated through the IoT devices through the remote database server which is present on the cloud. The cloud computing platform that is used for this synchronization classifies the public data received into public data such as patient's ID and blood group and private data such as DNA. Once the data is processed, the final output is presented using visualization through a graphical user interface. The information that is collected through this system can be very vital for medical researchers who can use the visualizations to identify the patterns and detect the approaching diseases which can be useful in taking proactive actions for the improvement in the health of the patient tracked (Niewolny, 2013).

The smart gateway used in this system is the key attraction of the same as it provides authentication and authorization for securing end users. The key objectives of a gateway are to provide support for different protocols and enable communication between different devices. Besides these standard gateway services, smart gateway also provides other advanced services such as local repository for information storage, local processing of data captured through the sensors, enhancing services like data aggregation, fusion, and interpretation. UT gate is an example of a smart gateway which consists of Dual Core ARM-Cortex A9 cores with processing speed of up to 1.2GHz for each core and provides support for Ubuntu OS and 128 GB memory. Intel also provides some intelligent gateway options that can provide data delivery, data encryption, local decision making, and locking for software security. Some of the fast processors that can be used for providing these services include Quark SOC X1000/ X1020D and Atom E3826 processor.

Traditional security architecture used for IoT networks mainly rely on a centralized server which puts constraints on device security. However, the smart security architecture, many of these constraints are removed such that more secure and efficient architecture through the distributed approach can be provide with authentication and authorization added in the gateway. Even the restrained IoT devices can be provide with essential security provisions through the smart gateway such that the communication initiated or received by the end users can be secured. For this, the gateway acts on the behalf of the medical devices for establishing security (Sermakani, 2014).

Unlike Traditional gateways, smart gateways use local databases for the storage of sensing information and thus, the data can be processed locally. Thus, it acts as an embedded server for the constrained medical devices. The authentication and authorization responsibilities can also be broken down into distributed health gateways. There can be exclusive gateways that can handle the remote end point security needs. With this multi-domain network, attacks like Denial of Service can be disrupted in the SEA architecture. For the implementation of authentication and authorization in the networks, security protocols can be re-used. Healthcare devices do not have sufficient hardware to provide secure communication facilities with advanced security protocols and certificate validation used.

The smart e-health gateway connects remote users and the constrained IoT devices and contains an inbuilt IP based security protocol called Database Transport Layer Security (DTLS) (R & Arockiam, 2016).

4.2.5. Datagram Transport Layer Security

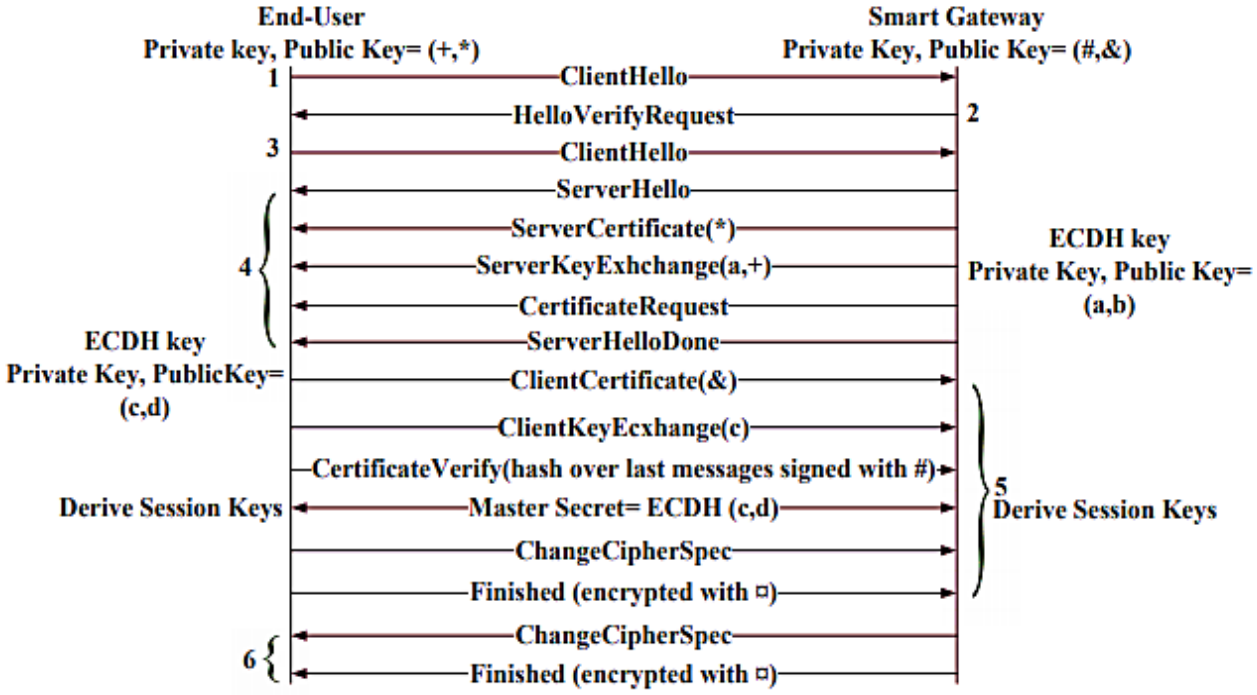

Figure 19: DTLS (Kim, 2014)

DTLS is a main handshake protocol used in secure IoT architecture. The handshake begins with a ClientHello message which has security parameters stored that are used at the later stages for computing of the pre-master secret key. Flight 3 has an additional cookie received from ClientHelloVerify and Flight 4 has ServerHello message containing the cipher suite starting the current handshake. A HandshakeFailure message is sent as an alert when communication fails. The public key is generated using OpenSSL 1.0.1. version which is open source project used for the implementation of the Software Security Layers, TLS, and cryptographic libraries such as hash algorithms, public key, and symmetric keys (Kim, 2014).

The end of the flight 4 is marked by an announcement with ServerHelloDone message and the first message in the flight 5 begins with the mutual authentication of the security certifications from the end users. Additional parameters may be needed in certain cases for generating the master key for which ClientKeyExchange message can be used. CertificateVerify message proves that the smart gateway contains the private key that corresponds to the certificate's public key. Agreed cipher suits may be used for encryption of the messages for which ChangeCipherSpec message is sent. Once all flight messages have been encrypted, a finished message is sent marking the completion of the handshake. In the next flight that is flight 6, the gateway would respond to these messages such that peers on both sides of the gateway would agree to send and receive the messages. A mutual authentication is done between the end points and the smart gateway. Within a DTLS handshake, smart gateway authenticates the end points in this way using security certificates. For this to happen, the gateways contain a set of trusted security certificates that are used for authentication from one side. Authentication can happen either using the handshake mechanism or application level protection. Smart gateway can control the communication happening between the end user and the smart gateway so that it is more secured as compared to the regular gateways. Once the mutual authentication is completed, the end user gets authorized as a trusted user and the data would get transferred between sensor devices through the gateway (Preethi & J Senthil Kumar, 2017).

4.2.6 IoT based secure healthcare system using Body Sensor Network

Security and privacy issues are most important to understand in the Body Sensor Network that is IoT based. The confidentiality of the healthcare system can be taken care of by using lightweight authentication protocols and encryption. A BSN based healthcare system can be used for accomplishing security requirements of the system. The system involves checking of workflow compliance across the five key elements that include data, activities, location, time limits, and resources. Rules are set for activities related to what may be performed by what object and by which roles. These rules can also prescribe appropriate sequence in which activities are required to be performed. Petri net patterns and usage

control policies are used for formalization of these rules and obligations related to activities. The rules can then be integrated using the procedural workflows which would act as a security automata. Compliance related rules can be organized into categories based on their semantics and entities so that usage control can be established.

A secure Body Sensor Network based IoT healthcare system can have standard modules for login, registration, key authority control, Local Process Unit (LPU), and Body Sensor Network care server. Figure 20 shows the different components of a secure IoT based Body Sensor Network.

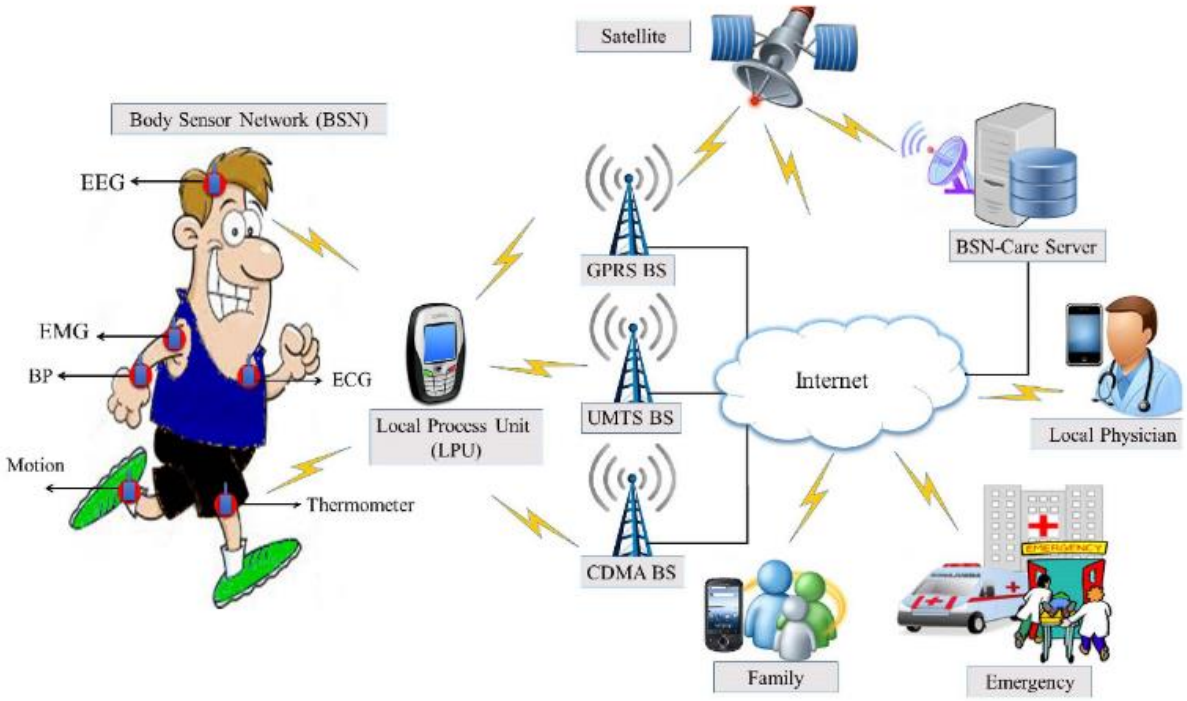

Figure 20: Secure IoT-based modern healthcare system using BSN (Gope and Hwang, 2016)

Login is used for gaining access to an application sitting in a remote computer through the use of a secure user ID and a secure password such that when a correct combination is entered will the user be sent to the administration page. Registration module has personal care details of the patient, physician, family, and emergency contacts. Each of these users are provided with their respective IDs that would be used for searching database

and conducting reviews. Key authorities are the centers used for generating public and private keys. These key authorities can have one central and more than one local authorities addressed. Each local authority would be made responsible for the management of different set of issues and attributes. They will also give differential rights of access to different users. LPU sends the updates to the BSN care system periodically and the servers confirm its identity using the authentication protocol. Once this authentication is done, the LPU can interact with the BSN care server which receives the data about patients and other people from the LPU through the bio sensors. BSN data is fed into the backend data base and the data retrieved from the same is analyzed. The interaction can involve patients, their family members, physicians and emergency units that are located nearby. An action table is maintained by the care server for very category of the BSN data received from LPU.

The system uses a functional encryption called Attribute Based Encryption (ABE) for generating public keys as it has the benefits of high level of security, efficiency, and flexibility. In this scheme, the cipher texts carry descriptive values that secret keys associate with. A function is used for determining a user and the respective key that is needed to learn from a cipher text. In ABE, keys and cipher texts are associated with access policies. Key is used for decrypting the cipher text when associated attributes of the cipher text satisfy the access policies. ABE systems can be Cipher text-Policy ABE (CP-ABE) in which cipher texts associate with access polices and keys with attributes or Key-Policy ABE (KPABE) in which keys associate with access policies and cipher texts with attributes. An ABE system us constructed based on the suitability of the type to the access policies and the attributes.

Access policies are defined using linear secret schemes or Boolean formulas and thus, have a high level of flexibility with a rich structure that allows a large space for the storage of attributes and cipher texts. However, this presents security challenges as the messages are not individually authorized thus, several users can actually decrypt the messages that should not be the case. An attacker can collect multiple keys for attempting decryption of the cipher text. A scalable and better access control for the patient health records can use ABE technique for encrypting every patient data to overcome this challenging and enhancing the protection of the system. A data outsourcing center may be use for multiple data owner

scenarios defined for managing the complexities that exist between different types of users. This can ensure that a high level of privacy can be achieved for the patient by the development of the multi-authority ABE and using EC-MAABE.

BSN based secure IoT healthcare network can fulfil some of the security requirements of the system including mutual authentication, anonymity, secure localization, resistance to replay attacks, and data security. The LPU is authenticated by the server by verification of its one time alias identity, a tracking number, and parameters inside request message. Even if the synchronization is lost, shadow identity can still be used for authentication. While on one side the server authenticates the LPU, on the other side, LPU also have the rights to authenticate the server using V2 parameter that must match. With this feature, the need of mutual authentication is achieved.

In the BSN based healthcare scheme, the shadow identity and the one time alias identity used with the track sequence numbers can address the issue of anonymity which is another requirement for security in IoT based healthcare systems. The pair of shadow ID and the emergency key would need excessive storage in LPU as well as the healthcare server and thus, it is used only when dealing with a DOS attack that can happen in the event of the loss of synchronization between LPU and the healthcare server. This scheme can also be effective to prevent eavesdropping as in the event of interruption of the response message, LPU would not be able to receive the signal in the desired time period.

Estimating the location of the patient is important in health care application in the real time. An attacker can intervene with the process and send a wrong location about the patient to the server through the use false signals. This problem can be overcome by the BSN based secure healthcare system scheme with the anonymous authentication. When the server needs to know the location of a patient, an encoded identity of the location would be sent to it that would be decoded to reveal the physical connection. With this encoding and decoding procedure, the location of the patient is secured from the unauthorized users or attackers.

Another way an attacker can compromise a system is by replaying a message already sent for passing the verification process. However, this interruption is avoided in the BSN based protocol as it does not allow any MA 1 message request to be sent twice. In case, a

sender tries to do that, the recent track sequence number would allow the server to detect the attempt. On the side of the LPU also, the attempt would get recognized as V2 parameter value would not match with the message.

CISCO Healthcare Network

One of the most important qualities of CISCO healthcare network is that it is based on developing engagement with the patients along with identifying solutions through which data can be made safe and secured. Therefore, the purpose is to provide empowerment to the patients regarding the ways in which they can improve the safety and security of their data. In order to improve the service provided to the users along with improving the security of the data and information system, CISCO has also entered into collaboration with iOS to further improve the quality of its healthcare information system. The important element of CISCO healthcare network is that it also provides guidance regarding the patient care and the team of workers that is needed to be maintained in order to fulfill the future needs of the patients (CISCO, 2018).

4.3 Process Solutions

4.3.1 FDA guidance on medical devices

FDA has issued certain guidelines for the use of medical devices for the protection of the patients and the users of these devices. These guidelines are required to be followed while designing security solutions for healthcare. The guidelines provide details of how safety communication for the hospital networks must be carried out and makes recommendation for manufactures and healthcare organizations for identifying safeguards that can help reduce the chances of failure of a medical device due to a cyber-attack. Certain guidelines have been provided on what healthcare facilities should do.

Healthcare facilities are required to put restrictions on access to healthcare data based on the authority such that unauthorized personnel cannot access the data. Further, they must have the levels defined for risks so that decisions can be taken to act on priority based on the level of risk. Risks can be low level that are classified as Class 1. Such risks would not

demand an immediate action. Class 3 risks called high risks on the other side would demand immediate action as they are likely to affect human life by causing impairments to health, injuries or illnesses. Devices are assessed on the basis of factors like trust, identity, privacy, and security (TIPS). A device can have low, medium or high level of requirements for each of these TIPS categories. Devices that may have low TIPS requirements include wearables like Fitbit. Some devices can have high TIPS requirements such as pacemaker and insulin pump (Schorer & Spier, 2017).

One guideline of FDA demands participation of various stakeholders in the system for improvement of the security. These stakeholders can include the healthcare service providers, manufacturers of the patients' devices, and healthcare facilities. The defense system needs to be set in depth such that security is maintained at multiple levels of the software using antivirus and updated firewalls. The facilities must provide a system for monitoring network activities such that the unauthorized use of the network and the healthcare system can be spotted. If in the routine inspection, network components are observed to be compromised then immediate action must be taken. Moreover, the security patches must be regularly updated and unnecessary or unused ports as well as services must be disabled. If a security problem arises with respect to cybersecurity with a medical device, the device manufacturer may be contacted for resolution. Alternatively, FDA or DHS ICS-CERT can be approached by the healthcare system provided for reporting the vulnerability and getting the resolution of the threat.

As per FDA guidelines, the healthcare organizations must have specific strategies for maintaining functionalities of the system during adverse conditions like a security attack. FDA provides both pre- and post-market guidelines on the use of medical devices but these are only the guidelines and not enforceable. However, there are certain Federal laws that provide some level of protection for the consumer data as they mandate the company to protect the patient information and any data that is being kept in possession. Acts like GLBA, Fair Credit Transactions Act/Fair Credit Reporting Act, HIPAA/HITECH ACT, Telephone Consumer Protection Act and Child Online Privacy Protection Act are

enforceable by regulatory authorities like FDA, FTC, FCC, and SEC (A.kavimani & F.Anishya, 2017).

There are three states in US including Texas, MA, and CA that have comprehensive security programs in written that include procedures for data breach notification to law enforcement agencies, insurance regulator, and credit reporting agencies as well as the individuals affected. These notifications should go in the form of disclosures with details of risks and the harm it could cause. There are data protection laws that work to protect SSN numbers, Patient Health Records, and Employee records demanding protection of them. Some state laws also have provisions for data destruction that allow consumers to take private actions against the healthcare organizations if they fail to protect the patient data. If such an action is taken, the law provides support for recovery for victims on specific vases. There have been 70 lawsuits filed between December 2013 and January 2014 when Target breach had affected the data of consumers and financial institutions. Sony picture had faced lawsuits from former employees in Alabama and California for the same data breach (Kammuller, Augusto, & S, 2016).

4.4 Justification of Using IT solutions

The rationale behind the use of IT strategies is not only to identify the problems but also the solutions that can be applied in relation to dealing with the issues related to IT security. However, further solutions are also needed to be identified in relation to improving the overall IT safety and security practices. Therefore, it is imperative that organizations develop a kind of business strategy that would be helpful in terms of developing IT safety and security. The choice of four techniques at the initial stage was made after conducting in-depth analysis and evaluation regarding the utilization of these techniques along with the elements associated with them. The careful analysis of these techniques provided an opportunity to ensure that they have the capability and the strength to deal with different kinds of solutions with respect to maintaining the security of information regarding patients.

Chapter 5. Discussion

5.1 Deduction

The author commenced his research by first, collecting different sources of information about IoT based healthcare systems and security. These sources were journals, research papers, essays, books and conference papers. They were then critically reviewed and the research approach of epistemology (hypothetical deductive approach in specific) as discussed in chapter 3 was employed to shortlist important pieces of information. After the extraction of data from various, authentic educational and informative mediums, both online as well as hardcopies, the author shortlisted a few high-profile security systems including CodeBlue, Elliptical Curve Cryptography, TinySec, Datagram Transport Layer Security Architecture and IoT-based Body Sensor Network.

5.1.1 Addressing research questions

An elaborate discussion of the systems listed above was able to adequately answer the questions raised in the beginning of the research paper. One of these questions was:

How do IoT based healthcare systems work?

The answer to this question can be found in Chapter 4 which discusses in detail the technical features and working mechanism of each security system. Another concern that the underlying analysis of these systems addresses is:

'How can healthcare systems be made secure with the use of the right IoT architecture?'

For instance, when storage constraints are significant ECC is a preferable encryption methods, or where tangible, wireless patient sensors, delivering sensitive personal information are involved the answer is TinySec!

After a thorough analysis and research on each of these systems the author found out that they varied on the basis of type; i.e. a protocol, an encryption method, an architecture, a network or an algorithm etc. as well as their usability which was largely dependent on their key features. CodeBlue is a sophisticated sensor network with features like ad hoc deployment, publish/subscribe communication and concurrent query handling and is particularly useful for emergency conditions (Shnayder et al., n.d.). Elliptic Curve Cryptography is an algorithm that offers smaller keys and lower CPU and memory consumption (Stolbikova, 2016). TinySec is a layered architecture providing message integrity, confidentiality, portability and replay protection. DTLS is a protocol that allows datagram-based applications to communicate in a secure way by preventing data eavesdropping, tampering, or message forgery (IoT ONE, n.d.). Lastly, the author has discussed a body sensor network that can effectively address issues of data modification, impersonation, eavesdropping, tracking and replaying (Gope and Hwang, 2016). A more detailed discussion of these systems is given in the section below.

5.2 Analysis

Whether they are healthcare related digital equipment (insulin delivery coagulation testing), patient monitoring (ingestible sensors, cancer trackers) or IoT based security

handling sensitive information, IoT has penetrated the healthcare industry, to reduce healthcare expenditure and provide better facilities. This argument is supported by the evidence that by 2019 approximately 87% of healthcare organizations will have adopted IoT based healthcare technology (I-scoop.eu., n.d.). Figure 18 shows the breakdown of healthcare domains where IoT is being actively used. Telemedicine is the use of IoT devices including smartphones and applications to diagnose and treat patients. Medical management can include the storage, management and organization of patient information, past health records, prescriptions and medical history. Cardiology and radiology are important clinical procedures that are now largely IoT-based while a patient's blood pressure, body temperature, glucose level, insulin intake etc. can also be monitored using IoT devices. Connected Imaging is another secure communication network, a portal where patients and doctor can interact through exchange of informative images, an example of which is X-ray results.

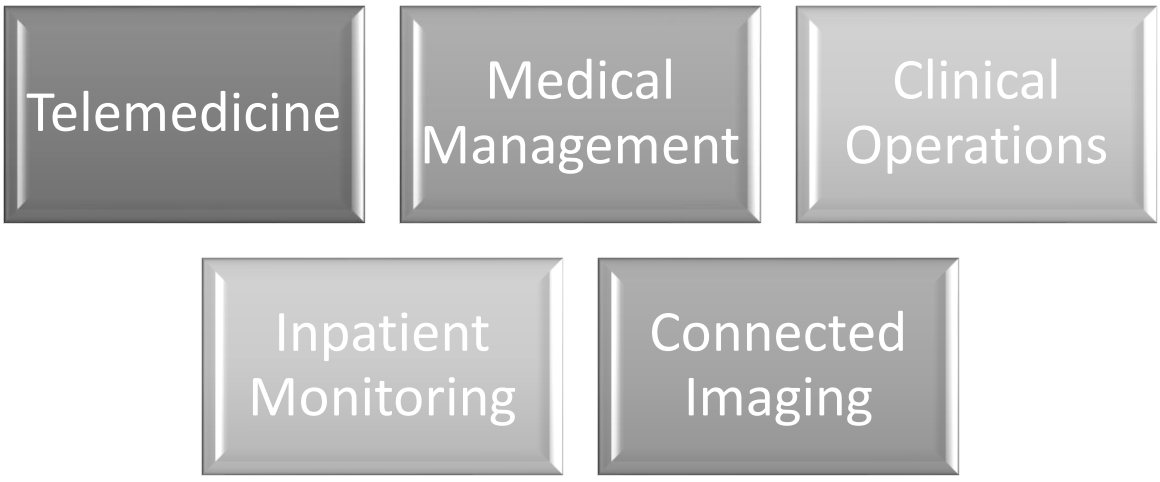

Figure 21: IoT in Healthcare

IoT healthcare can help boost patient engagement, medical care, patient data integrity and accessibility to healthcare facilities. It has been observed that the most popular element of IoT healthcare are IoT based applications and devices, which indicates a higher consumer consciousness. Next in priority are IoT based security systems which ensure confidentiality, authenticity and reliability of a user's information. However, a significant drawback of using IoT for security of sensitive patient information is its susceptibility to cyberattacks and implication of stringent regulation laws that limit its versatility. Evidence indicates that the use of IoT has also encouraged remote monitoring to become more common instead of binding patients in a hospital environment. This means higher level of comfort and ease for a patient enabling him to get 'back on track' and a reduction of expenditure for hospital facilities.

5.2.1 Advantages and disadvantages of chosen systems

The different security systems for healthcare management that the author has investigated and discussed in this dissertation have both advantages and disadvantages. For example where BlueCode offers robustness, scalability, discovery protocol, ad hoc networking, publish/subscribe communication and simultaneous query handling, bandwidth limitations are a serious issue (Shnayder et al., n.d.). Providing prioritized traffic and reducing energy consumption is also a critical issue (Malan et al., 2004). Similarly, Elliptical Curve Cryptography is useful in terms of CPU and memory consumption, in smaller length keys and rapid reassigning of keys. However, an incorrect implementation of an ECC key

can lead to data leakage. An ECC system is vulnerable to many different types of attacks including timing attacks and power attacks. In a timing attack the attacker measures the difference in the time of occurrence of peaks of power consumption to determine the private key. However in a power attack the actual shape and amplitude of the peaks is observed (Canteaut, Lauradoux and Seznec, 2006). TinySec might be capable of providing message integrity, confidentiality and authenticity but it cannot protect the system from resource consumption attacks, physical tampering, and node capture attacks as mentioned earlier as well. DTLS, although offers high levels of message security and confidentiality and saves significant code space, has to deal with packet reordering and loss of data larger in size than a datagram network packet (IoT ONE.,n.d.). However, despite these deficiencies and drawbacks each of these systems are claimed to provide high levels of security, provided they are implemented correctly and efficiently. For example the implementation of CodeBlue project in a hospital improved the overall survival rate by 26% and cardiac arrest rate by 11.3% by making immediate emergency calls and recalling existing authentic medical records of patients (Dhar et al., 2018). Similarly after a series of experiments spanning over 30 years ECC has finally rose from a theoretical reasoning to actual implementation in security networks. Similarly, TinySec secures a superior psotion amongst most WSN protocols. On the other hand, introduction of IoT in BSN has adequately addressed issues of data eavesdropping, modification and replaying. This implies that despite the noticeable shortcomings of the afore-mentioned security systems, they are outweighed by their countless benefits.

The answer to the research questions have been made on the basis of the information regarding the ways in which IoT system works which is one of the major elements of the research questions. There were some other ways as well that were used to answer the question of this particular research such as the type of architecture that is needed to be used to increase the confidentiality and reliability of the information system along with addressing the security issues and concerns. The information about reliability was obtained by means of increasing the overall safety and security of the IoT architecture. The combination of all these elements was important in terms of not only answering the questions of the research but was also helpful in providing guidance regarding the ways in which security and the reliability of the information can be maintained.

Chapter 6. Conclusion

Despite the several security and privacy threats posed by IoT technology, systems and protocols have simultaneously been developed to prevent and overcome these breaches and provide a safe storage for personal health data. This has led to the evident popularity of IoT based healthcare whether they are wearable devices, services or databases. In fact statistics have revealed that the use of IoT is poised to rise at an accelerated rate (Jain, 2018).

6.1 Addressing future gaps in IoT Healthcare

It is not a fact unknown that IoT has taken the world by a storm and woven itself into our lives, including the healthcare and medical industry. However, the freedom and accessibility provided by IoT, is not free from deficiencies. Addressing these gaps in future can completely reinvent the scope of IoT in healthcare.

One such matter of concern is that today everyone is on the internet and what isn't on the internet does not exist. More users are synonymous to an increased amount of data, handling which would eventually become extremely challenging. This can greatly jeopardize the security of personal information. Interpreting results from such a large amount of data is a tedious job that requires more sophisticated analytics programs and data experts than what currently exist.

Multiple device integration is another shortcoming that manufacturers are currently working on. The increase in the number of users has been exponential and the trend is expected to continue in future. Therefore, it is imperative that a set of protocols and standards are designed that allow easy grouping of devices and speedy sharing of information. This could greatly accelerate the treatment process and deliver complete well-rounded information to medical officers.

6.2 Future Developments of IoT in Healthcare

Table 2 refers to a few IoT based healthcare devices and applications expected to be released in future, along with their capabilities and possible benefits.

IoT based device/application/service	Features	Benefits
HOMNI (Sarang, 2018)	Monitors a user's sleep environment. Tracks sleeper's movement and sends to an application.	Helps determine how well an individual has slept Help cure patients with sleeping disorders
Vuzix Blade (Sarang, 2018)	Smart glasses that can connect to Google Alexa. Sends email and text notifications via Bluetooth	Beneficial for immobile personnel
Robotic Engineering (Sarang, 2018)	Medicine delivery Food delivery Supplies Delivery	Beneficial for house-bound patients and hospital staff

Table 2: Future IoT devices

Other future developments in the context of IoT can include developing the already existing security systems that have been discussed in this dissertation. For example according to Shnayder et al., (n.d.) reliability mechanism can be introduced to the communication layer of the CodeBlue prototype. Another area of development can be resolving the bandwidth limitation by allowing nodes to share the bandwidth across each other. Each CodeBlue query could specify a data priority that would allow some messages (say an alert for a patient emergency) to be placed at a higher priority. Maleh and Ezzati (2016) have taken the DTLS protocol to the next level and proposed an enhanced cryptography protocol that has a better performance in terms of packet overhead, handshake time duration, size and energy consumption.

6.3 Importance of IoT in Healthcare

It is crucial to understand that where security is a serious issue in other IoT related fields, it can be a matter of life and death in medicine. In fact privacy has been ranked as the highest in IoT security concerns (Help Net Security, 2015**).**Whether it is directly controlling a medical equipment or data hostage for financial benefit, privacy breaches can prove to be detrimental for patients and doctors alike. While several protocols, high-profile security systems have been designed, some of which have been discussed in this dissertation and are being actively employed for privacy and confidentiality purposes, IoT security for the health sector is still in a critical condition. This is due to a unanimous lack of concern about the issue, or the lack of security expertise in this field. Similarly manufacturers consider security as a service or a luxury that needs to be outsourced from an IT expert instead of being a key feature of the device.

6.4 Importance of thesis research in IoT for Healthcare

The research and the findings obtained through this thesis could be utilized and analyzed to develop further solutions regarding the management and security of information systems within the healthcare industry. It is expected that the findings of the research would pave the way towards further identification of the solutions as well as the challenges associated with maintaining the security of the information systems. Therefore, it is expected that the research can make a positive impact towards taking measures related to protecting the health information systems.

The findings of the research can be used by healthcare professionals in order to improve the safety and security of the information system. Furthermore, the findings of the research can also be utilized by the academic professionals and the researchers in order to conduct further knowledge regarding the ways in which safety of the healthcare information system can be ensured. Therefore, it can be stated that the findings of the research would be beneficial for the patients, providers of healthcare service along with the researchers in the future. The other important quality of this entire research is that it will also provide guidance regarding the future security challenges that can arise in relation to maintaining the security

of the information and data in information security system. This is because of the detailed analysis that has been carried out within the research regarding the security and privacy issues of the data and the impact that they have on the safety of the entire information system. In addition to that, techniques will also be identified regarding the ways in involvement of patients can be ensured within this entire system,

References

Aggarwal, R. and Das, M. (2012). RFID security in the context of "internet of things." *Proceedings of the First International Conference on Security of Internet of Things - SecurIT '12*.

A.kavimani, & F.Anishya. (2017). A Secure Healthcare System using IoT device and Body Sensor Network. *Asian Journal of Applied Science and Technology (AJAST)*, 1(5), pp.183-189.

Abbasi, M. A., Memon, Z. A., Syed, T. Q., Memon, J., & Alshboul, R. (2017). Addressing the Future Data Management Challenges in IoT: A Proposed Framework. *(IJACSA) International Journal of Advanced Computer Science and Applications, 8*(5), pp.197-207.

Aroul, A. L., Walker, W., & Bhatia, D. (2004). *A Framework for Patient Monitoring.* University of Texas at Dallas.

Bachhav, S. (2018). *IoT Based Real-Time Remote Patient Monitoring System - Bitware Technologies*. [online] Bitware Technologies. Available at: https://bitwaretechnologies.com/IoT-based-real-time-remote-patient-monitoring-system/ [Accessed 19 Sep. 2018].

Bagot, M., Launay, P., & Guidec, F. (2016). *A Flexible Architecture for Mobile Health Monitoring.* HAL.

Bardach, S. H., Real, K., & Bardach, D. R. (2015). Perspectives of healthcare practitioners: An exploration of interprofessional communication using electronic medical records. *Journal of Interprofessional Care*, 31(3), pp. 300-306.

Beiske, B. (2007). Research Methods. Uses and Limitations of Questionnaires, Interviews, and Case Studies.

Begum, S., & Parveen, H. (2016). U-HEALTHCARE and IoT. *International Journal of Computer Science and Mobile Computing*, 5(8), pp. 138-142.

Begum, S., & Venugopal. (2016). Comparison of various techniques in IoT for Healthcare System. *International Journal of Computer Science and Mobile Computing*, 5(3), pp. 59-66.

Bilal, M. (2012). *A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers.* Zhejiang University Hangzhou.

Bourouis, A., Feham, M., & Bouchachia, A. (2012). A New Architecture of a Ubiquitous Health Monitoring System: A Prototype of Cloud Mobile Health Monitoring System. *IJCSI International Journal of Computer Science Issues*, 9(2), pp. 434-444.

Bozdogan, Z., & Kara, R. (2015). Layered model architecture for internet of things. *Journal of Engineering Research and Applied Science*, 4(1), pp. 260-264.

Canteaut, A., Lauradoux, C. and Seznec, A. (2006). *Understanding cache attacks*. [online] Institut National de Recherche en Informatique et en Automatique. Available at: https://www.rocq.inria.fr/secret/Anne.Canteaut/Publications/RR-5881.pdf [Accessed 23 Sep. 2018].

CityPulse. (2014). *Real-Time IoT Stream Processing and Large-scale Data Analytics for Smart City Applications.* CityPulse.

Collins, K. (2015). *Know your real-time protocols for IoT apps*. [online] InfoWorld. Available at: https://www.infoworld.com/article/2972143/internet-of-things/real-time-protocols-for-IoT-apps.html [Accessed 16 Sep. 2018].

Davidavičienė, V. (2018). Research Methodology: An Introduction. *Progress in IS*, pp.1-23.

Dasgupta, A., Mehta, R., & Raha, D. (2012). *Healthcare Infrastructure and Services Financing in India: Operation and Challenges.* PWC.

Denzin, N. and Lincoln, Y. (2000). *Handbook of qualitative research*. Thousand Oaks: Sage.

Dhar, M., Monangi, S., Setlur, R., Ramanathan, R. and Bhasin, S. (2018). Analysis of functioning and efficiency of a code blue system in a tertiary care hospital. *Saudi Journal of Anaesthesia*, 12(2), p.245.

Dlodlo, N. (2013). *Potential applications of the internet of things technologies for South Africa's health services.* Meraka Institute.

eeNews Europe. (2016). *RFID-based sensors as a data source for the IoT*. [online] Available at: http://www.eenewseurope.com/design-center/rfid-based-sensors-data-source-IoT/page/0/1 [Accessed 19 Sep. 2018].

En.wikipedia.org. (n.d.). *Internet of things*. [online] Available at: https://en.wikipedia.org/wiki/Internet_of_things [Accessed 16 Sep. 2018].

Espina, J., Falck, T., Panousopoulou, A., Schmitt, L., Mülhens, O. and Yang, G. (2014). Network Topologies, Communication Protocols, and Standards. *Body Sensor Networks*, pp.189-236.

Fujitsu, S. (2016). *Real Time IoT Tracking and Visualization.* Intel.

G, V., & A, B. M. (2016). Security Challenges in IoT Applications in Healthcare Domain. *International Journal of Advances in Electronics and Computer Science*, pp. 141-144.

Garg, A. (2016). *The Internet of Things: Impacts on Healthcare Security and Privacy.* Litmos.

Garg, R. (2017). *Digital and Information technology - Standardization National and International Scenario.* International Standards Conclave.

Gawdan, I. and Sarhan, Q. (2016). Performance Evaluation of Novel Secure Key Management Scheme over BAN Wireless Sensor Networks. *Journal of University of Duhok*, 19(1), pp.179-188.

Gope, P. and Hwang, T. (2016). BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network. *IEEE Sensors Journal*, 16(5), pp.1368-1376.

Grandviewresearch.com. (n.d.). *Wearable Technology Market Size, Share | Industry Trends Report, 2022*. [online] Available at: https://www.grandviewresearch.com/industry-analysis/wearable-technology-market [Accessed 30 Aug. 2018].

G3ict.org. (n.d.). *Internet of Things: New Promises for Persons with Dsiabilities*. [online] Available at: http://www.g3ict.org/download/p/fileId_1025/productId_335 [Accessed 19 Sep. 2018].

Help Net Security. (2015). *Top IoT concerns? Data volumes and network stress - Help Net Security*. [online] Available at: https://www.helpnetsecurity.com/2015/12/09/top-IoT-concerns-data-volumes-and-network-stress/ [Accessed 21 Sep. 2018].

Hou, Y., Li, M. and Guttman, J. (2013). Chorus. *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec '13*.

H.Weber, R. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), pp. 23-30.

Human Kinetics Europe. (n.d.). *Steps of the research process*. [online] Available at: https://uk.humankinetics.com/blogs/excerpts/steps-of-the-research-process [Accessed 21 Sep. 2018].

infisim, V. (n.d.). *What are the main benefits of IoT in healthcare? | InfiSIM*. [online] InfiSIM. Available at: https://www.infisim.com/main-benefits-IoT-healthcare/ [Accessed 16 Sep. 2018].

Internet of Things (IoT). (2017).*This will help the Internet of Things growing faster....* [online] Available at: http://nicolaswindpassinger.com/IoT-standardization-care [Accessed 21 Sep. 2018].

IoT Agenda. (n.d.). *What is IoT devices (internet of things devices)? - Definition from WhatIs.com*. [online] Available at: https://internetofthingsagenda.techtarget.com/definition/IoT-device [Accessed 16 Sep. 2018].

IoT ONE. (n.d.). *Datagram Transport Layer Security (DTLS) | IoT ONE*. [online] Available at: https://www.IoTone.com/term/datagram-transport-layer-security-dtls/t167 [Accessed 21 Sep. 2018].

I-scoop.eu. (n.d.). *Internet of Things (IoT) in healthcare: benefits, use cases and evolutions*. [online] Available at: https://www.i-scoop.eu/internet-of-things-guide/internet-things-healthcare/ [Accessed 4 Sep. 2018].

Islami, S. M., D. K., Kabir, H., Hossain, M., & Kwak, K.-S. (2015).The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, Volume 3, pp. 678-708.

ISO. (2014). *Internet of Things (IoT) Preliminary Report.* ISO.

ISO. (2018). *Information technology – Internet of Things Reference Architecture (IoT RA).* ISO.

Jain, Y. (2018). *13 IoT Statistics Defining the Future of Internet of Things*. [online] Newgenapps.com. Available at: https://www.newgenapps.com/blog/IoT- statistics-internet-of-things-future-research-data [Accessed 30 Aug. 2018].

Kahraman, E. (2010). *Evaluating IT security performance with quantifiable metrics.* Institutionen for Data-och Systemvetenskap.

Kammuller, F., Augusto, J. C., & S. J. (2016). *Security and Privacy Requirements Engineering for Human Centric IoT Systems using eFRIEND and Isabelle.* Middlesex University London.

Karlof, C., Sastry, N., Wagner, D., & Ruggieri, P. (2017). *TinySec: A Link Layer Security Architecture for Wireless Sensor Networks.* Semantics Scholar.

Kim, J. T. (2014). Privacy and Security Issues for Healthcare System with Embedded RFID System on Internet of Things. *Advanced Science and Technology Letter*, Volume 72, 109-112.

Kodali, R., Swamy, G. and Boppana, L. (2017). An implementation of IoT for healthcare. In: *Conference: 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*. [online] Warangal: IEEE. Available at: https://www.researchgate.net/publication/305284960_An_implementation_of_IoT_for_healthcare [Accessed 16 Sep. 2018].

Kolozali, S. (2014). A Knowledge-based Approach for Real-Time IoT Data Stream Annotation and Processing. IEEE International Conference on Internet of Things.

Konsek, H. (2015). The Architecture of IoT Gateways - DZone IoT. [online] dzone.com. Available at: https://dzone.com/articles/IoT-gateways-and-architecture [Accessed 16 Sep. 2018].

Kube, M., Bessin-Py, S., Taubert, J. and Benkoel-Adechy, D. (2017). *How the IoT is helping people living with disability - Gemalto blog*. [online] Gemalto blog. Available at: https://blog.gemalto.com/IoT/2017/07/27/IoT-helping-people-living-disability/ [Accessed 19 Sep. 2018].

Lake, D., Milito, R., Morrow, M., & Vargheese, R. (2013). *Internet of Things: Architectural Framework for eHealth Security.* Cisco Systems.

Malan, D., Fulford-Jones, T., Welsh, M. and Moulton, S. (2004). CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. In: *International Workshop on Wearable and Implantable Body Sensor Networks*. [online] London. Available at: https://dash.harvard.edu/handle/1/3191012 [Accessed 23 Sep. 2018].

Maleh, Y. and Ezzati, A. (2016). Towards an Efficient Datagram Transport Layer Security for Constrained Applications in Internet of Things. *International Review on Computers and Software (IRECOS)*, 11(7), p.611.

Mallick, M. R. (2016). A Comparative Study of Wireless Protocols with LI-FI Technology: A Survey. *International Journal of Advanced Computational Engineering and Networking*, 4(6), pp. 123-127.

Milovanovic, D., & bojkovic, Z. (2017). Cloud-based IoT healthcare applications: Requirements and recommendations. *International Journal of Internet of Things and Web Services*, Volume 2, pp. 60-65.

Mishra, R. k., & Pandey, R. (2013). *Aspects of Network Architecture for Remote Healthcare Systems.* F.G.I.E.T .

Mohammed, J., Lung, C., Ocneanu, A., Thakral, A., Jones, C. and Adler, A. (2014). Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing. *2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*.

MS, A. (n.d.). *Elliptic Curve Cryptography*. [ebook] MIT University. Available at: https://ocw.mit.edu/courses/mathematics/18-704...elliptic-curves.../asarina.pdf [Accessed 21 Sep. 2018].

Mukherjee, S., Dolui, K., & Datta, S. K. (2013). *Patient Health Management System using e-Health Monitoring Architecture.* Kolkata, India: St. Thomas' College of Engineering and Technology.

Munir, A., Kansakar, P., & Khan, S. U. (2017). *IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things.* ARXIV.

Narendra, P., Duquennoy, S., & Voigt, T. (2015). *BLE and IEEE 802.15.4 in the IoT: Evaluation and Interoperability Considerations.* SICS.

Nath, S., & Som2, S. (2017). Security and Privacy Challenges: Internet of Things. *Indian Journal of Science and Technology*, 10(3), pp 2-5.

Niewolny, D. (2013). *How the Internet of Things Is Revolutionizing Healthcare.* Freescale Semiconductor.

Paavola, M. (2007). *Wireless Technologies in Process Automation - Review and an Application Example.* University of Oulu.

Patel, S., Singh, N., & Pandya, S. (2017). IoT based Smart Hospital for Secure Healthcare System. *International Journal on Recent and Innovation Trends in Computing and Communication*, 5(5), pp. 404-408.

Pathak, A. K. (2017). Security Challenges in Internet of Things (IoT). *International Journals of Advanced Research in Computer Science and Software Engineering, 7*(6), 648-652.

Preethi, 1. S., & J Senthil Kumar. (2017). IoT based Secure Healthcare System using BSN. *IJRSET*, 4(4), pp. 40-46.

Radio-electronics.com. (n.d.). *What is ZigBee | Wireless Networking Technology | Tutorial*. [online] Available at: https://www.radio-electronics.com/info/wireless/zigbee/zigbee.php [Accessed 16 Sep. 2018].

Raggett, D. (2016). *Tackling Data Security and Privacy Challenges for the Internet of Things.* Berlin: W3C.

Rahmani, A., Thanigaivelan, N., Tuan Nguyen Gia, Granados, J., Negash, B., Liljeberg, P. and Tenhunen, H. (2015). Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*.

Research-Methodology. (n.d.). *Positivism - Research Methodology*. [online] Available at: https://research-methodology.net/research-philosophy/positivism/ [Accessed 21 Sep. 2018].

Rfwireless-world.com. (2016). *IoT architecture basics | IoT architecture hardware, software*. [online] Available at: http://www.rfwireless-world.com/IoT/IoT-architecture.html [Accessed 29 Aug. 2018].

R, S. M., & Arockiam, L. (2016). A neoteric authentication scheme for IoT healthcare system, *International journal of engineering sciences & research technology*, 5(12), pp. 296-303.

Rudestam, K. and Newton, R. (n.d.). *Surviving your dissertation*.

Sajid, A., Abbas, H., & Saleem, K. (2016). *Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges.* Islamabad, Pakistan: National University of Sciences and Technology.

Sandoval, K. (2017). Securing Medical IoT devices. [Blog] *Nordic Apis*.

Sarang, R. (2018). *The Future of IoT: What to Expect From Our Devices This Year | McAfee Blogs*. [online] McAfee Blogs. Available at: https://securingtomorrow.mcafee.com/consumer/mobile-security/the-future-of-IoT-what-to-expect-from-our-devices-this-year/ [Accessed 16 Sep. 2018].

SathishKumar, J. and R. Patel, D. (2014). A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications*, 90(11), pp.20-26.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, (6th Ed.) London: Pearson.

Schorer, M., & Spier, M. (2017). *IoT Business Brief – Healthcare Business.* VMWare.

Sermakani, V. (2014). Transforming healthcare through Internet of Things. *Project Management Practioners Conference* (pp. 3-26). Bangalore: NIMHANS.

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, pp. 1-25.

Shen, W., Xu, Y., Xie, D., Zhang, T. and Johansson, A. (2011). Smart Border Routers for eHealthCare Wireless Sensor Networks. *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*.

Shimel, A. (2013). ECC and the CA Security Council, Making SSL and the Web safe today and tomorrow. [Blog] *Network World*. Available at: https://www.networkworld.com/article/2224044/opensource-subnet/ecc-and-the-ca-security-council--making-ssl-and-the-web-safe-today-and-tomorrow.html [Accessed 23 Sep. 2018].

Shoham, D. A., Harris, J. K., Mundt, M., & McGaghie, W. (2016). A network model of communication in an interprofessional team of healthcare professionals: A cross-sectional study of a burn unit. *Journal of Interprofessional Care,* 30(5), 661-667.

Shnayder, V., Chen, B., Lorincz, K., Fulford-Jones, T., Dawson-Haggerty, S. and Welsh, M. (n.d.). *CodeBlue: An Architecture for Medical Sensor Networks*. Cambridge: Division of Engineering and Applied Sciences, Harvard University.

Sidhu, B., Singh, H., & Chhabra, A. (2007). Emerging Wireless Standards - Wi-Fi, ZigBee and WiMAX. *International Journal of Electronics and Communication Engineering*, pp. 43-48.

Snieder, R. and Larner, K. (2013). *The art of being a scientist*. Cambridge: Cambridge Univ. Press.

Stolbikova, V. (2016). Can Elliptic Curve Cryptography be Trusted? A Brief Analysis of the Security of a Popular Cryptosystem. *ISACA Journal*, [online] 3. Available at: https://www.isaca.org/Journal/archives/2016/volume-3/Pages/can-elliptic-curve-cryptography-be-trusted.aspx [Accessed 23 Sep. 2018].

TechJini. (2017). *How IoT and Wearables Can Solve Today's Healthcare Challenges*. [online] Available at: https://www.techjini.com/blog/IoT-wearables-can-solve-todays-healthcare-challenges/ [Accessed 19 Sep. 2018].

The Economist Intelligence Unit Limited. (2018). What the Internet of Things means for consumer privacy. *The Economist*.

Torjusen, A., Abie, H., Paintsil, E., Trcek, D. and Skomedal, Å. (2007). Towards Run-Time Verification of Adaptive Security for IoT in eHealth. *Proceedings of the 2014 European Conference on Software Architecture Workshops - ECSAW '14*.

UKEssays. (2017). *Research Onion – Explanation of the Concept*. [online] Available at: https://www.ukessays.com/essays/psychology/explanation-of-the-concept-of-research-onion-psychology-essay.php [Accessed 21 Sep. 2018].

Us.sagepub.com. (n.d.). *https://us.sagepub.com/sites/default/files/upm-binaries/71809_Hoy_Chapter_1.pdf*. [online] Available at: https://us.sagepub.com/sites/default/files/upm-binaries/71809_Hoy_Chapter_1.pdf [Accessed 21 Sep. 2018].

V, R. B., & S, P. L. (2007). IoT Based Architecture for Patient Health Monitoring System. *International Journal of Innovative Research in Computer and Communication Engineering*, 5(5), pp. 10176-10181.

Wind. (2015). *Security in the Internet of Things: Lessons from the Past for the Connected Future.* Wind River Systems, Inc.

Zarghami, S. (2013). *Middleware for internet of things.* University of Twente.

Zhou, W., Zhang, Y., & Liu, P. (2018). *The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.* University of Chinese Academy of Sciences.

Zhou, X., & Lutfiyya, H. (2016). IoT Stream Analytics Platform. The University of Western Ontario.