Spring 5-5-2022

The Applications of the Internet of things in the Medical Field

Cody Repass

COLUMBUS STATE UNIVERSITY

The Applications of the Internet of things in the Medical Field

A THESIS SUBMITTED TO

THE D. ABBOTT TURNER COLLEGE OF BUSINESS

IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

TSYS SCHOOL OF COMPUTER SCIENCE

BY

CODY R. REPASS

COLUMBUS, GEORGIA

2022

The Applications of the Internet of things in the Medical Field

By

Cody R. Repass

Committee Chair:

Dr. Shamim Khan

Committee Members:

Dr. Lixin Wang
Dr. Jianhua Yang

Columbus State University
May 2022

THE APPLICATIONS OF THE INTERNET OF THINGS IN THE MEDICAL FIELD

A thesis submitted to The D. Abbott Turner College of Business in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

TSYS SCHOOL OF COMPUTER SCIENCE

by

Cody R. Repass

2022

Dr. Shamim Khan, Chair	5/10/22 Date
Lixin Wang Dr. Lixin Wang, Member	05/09/2022 Date
Dr. Jianhua Yang, Member	5/10/2022 Date

ABSTRACT

The Internet of Things (IoT) paradigm promises to make “things” include a more generic set of entities such as smart devices, sensors, human beings, and any other IoT objects to be accessible at anytime and anywhere. IoT varies widely in its applications, and one of its most beneficial uses is in the medical field. However, the large attack surface and vulnerabilities of IoT systems needs to be secured and protected. Security is a requirement for IoT systems in the medical field where the Health Insurance Portability and Accountability Act (HIPAA) applies.

This work investigates various applications of IoT in healthcare and focuses on the security aspects of the two internet of medical things (IoMT) devices: the LifeWatch Mobile Cardiac Telemetry 3 Lead (MCT3L), and the remote patient monitoring system of the telehealth provider Vivify Health, as well as their implementations.

INDEX WORDS: Cybersecurity, Internet of Things, IoT, Internet of Medical Things, HIPAA

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. Lixin Wang for his advice and assistance on this thesis. I would also like to thank the committee chair, Dr. Shamim Khan for his guidance. Most importantly, I would like to thank my loving wife, Michelle, who encouraged and supported me throughout, without whom this would not have been possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 0: Research Goal, Methodology, and Contributions

The research goal is to understand, identify, and analyze potential threats and vulnerabilities in the Internet of Medical Things (IoMT) devices, and provide an analysis of solutions to the issues identified from a cybersecurity perspective. Through the investigation of the Mobile Cardiac Telemetry 3 Lead and the remote patient monitoring kit from Vivify Health, a critical analysis of security issues and potential solutions is presented to reach the research goal.

IoMT is a growing application of IoT technology. It directly improves the quality of life of patients and eases the burden on healthcare providers. IoMT consists of IoT devices specifically developed to meet the needs of patients and healthcare facilities. IoMT is developed for remote patient monitoring, intensive care, and context awareness, which gathers information about a patient’s environment. IoMT can also be utilized beyond direct patient treatment, such as medical equipment and medication management.

I have conducted investigative analysis of two IoMT devices, the Mobile Cardiac Telemetry 3 Lead (MCT3L) and the remote patient monitoring kit from Vivify Health. I have formulated a series of questions to meet the research goal. These questions serve as the basis for the analysis of the IoMT environment. I met with a local hospital that provided the MCT3L User Guide, which contained the specifications for the MCT3L. I also met with Wellstar Home Health for a demonstration of the remote patient monitoring kit from Vivify Health. The information gathered from these sources provided me with the information to conduct analyses to fulfill the research goal.

My contributions to the field include the analysis of real IoMT devices, their threats and vulnerabilities, and solutions to further protect them. Furthermore, the work in this thesis illustrates the lacking security countermeasures found in IoMT devices currently deployed. This work contributes to the IoMT literature by conducting a thorough investigation of specific devices, the MCT3L, and the remote patient monitoring kit. The IoMT security literature is lacking in thorough technical examination of devices that are currently deployed. This work provides details of IoMT devices and the security risks they impose, along with a comprehensive analysis of possible solutions. These solutions consist of using secure communication protocols, using multi-factor authentication for user equipment, understanding the device manufacturer’s role in security, implementing robust security policies and procedures organization wide, utilizing network hardening techniques and network segmentation, providing IoMT security training and education, using lightweight security protocols, and using blockchain and cloud computing technologies.

Chapter 1: Introduction to the Internet of Things (IoT)

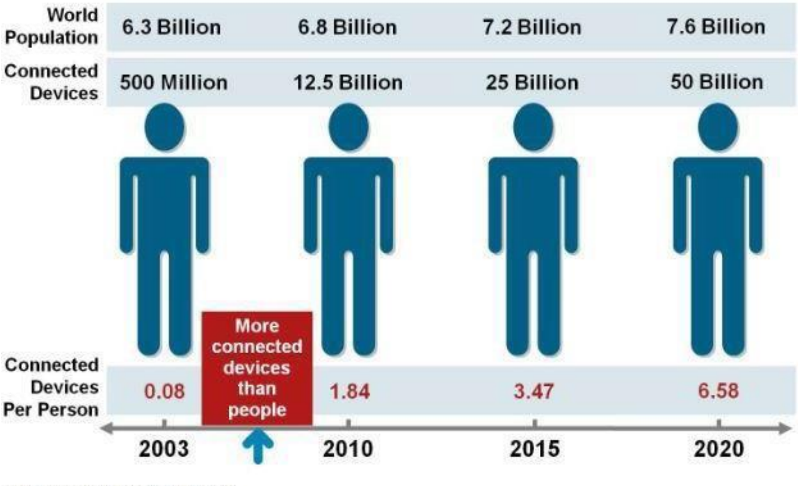
This chapter introduces the internet of things and its concepts and definitions. The background, applications, and elements of IoT are explored in this chapter. The basic concepts that make up an IoT system are discussed in-depth, which provides a foundation for the security issues and other challenges discussed in this thesis.

1.1 Definition and Background

The internet of things is a phrase that refers to the interconnectivity of physical objects to each other over networks [1]. There is not one standard definition that describes the internet of things, so using Cisco's definition, IoT refers to the fact that more physical devices, such as smartphones, are connected to the internet than people are [2]. These objects are able to collect and exchange information through communication protocols of existing network infrastructure. Ideally, IoT devices use sensors to collect and transmit information without human intervention, an intended seamless and hands-off process [1]. IoT is intended to give objects communication capability to make automated and smart decisions using the information collected and exchanged. IoT bridges together many different technologies to provide new and efficient applications [1]. How it works varies across its many uses, which is one of IoT's weaknesses.

The internet of things lacks a standard definition and body of standards [3]. IoT is heterogenous, meaning that there are many different technologies and implementations depending on its purpose. There is a ubiquitous number of languages and protocols in IoT, making it more difficult for standardization [3].

The phrase “the internet of things” was coined by Kevin Ashton in 1999 at MIT while developing radio frequency identification (RFID) technology [2]. Kevin Ashton referred to RFID as a precursor to IoT and believed that computers could keep track of and manage devices tagged with RFID sensors [4]. A modern example of this concept is quick response (QR) codes, digital barcodes that store information. The first ever internet-enabled appliance was a Coke machine at Carnegie Mellon University in 1982 [5]. The machine could detect the inventory and whether or not the drinks were cold [5]. While IoT existed as early as 1982, IoT technology did not come to full fruition until sometime between 2008 and 2009 [2]. Since then, the number of IoT devices has boomed. In Figure 1.1 below we can see just how many devices are connected to the internet compared to the world population.



Source: Cisco IBSG, April 2011

Figure 1.1: The Internet of Things Was “Born” Between 2008 and 2009 [2]

Looking at Figure 1.1, the number of connected devices increased by twenty-four times in the span between 2003 and 2010. To understand this boom, it is important to look at the evolutionary path of the internet. Gokhale, et al. [5] describe five eras of the internet: the internet of documents, the internet of commerce, the internet of applications, the internet of people, and finally the internetof things. Each step relates to an advancement of the internet’s capability and function. Beginning with simple document pages on the web, the internet advanced to commerce: shopping, banking, stock trading, etc.

Then the internet evolved where any user could create and participate on the world wide web, creating websites or writing blogs. The internet of people mainly refers to social media, people creating personal profiles and connecting with each other. Finally, we are at the internet of things, where physical, ordinary objects are given internet and communication capability. Since such a ubiquitous number of devices are connected, it is important to understand the many applications of IoT, and why it is a rapidly growing field of technology.

1.2 The Applications of IoT

The purpose of the internet of things, like most technology, is to make daily life easier and more efficient. This efficiency can be seen in many fields that utilize IoT. Today, IoT is a part of almost everything. Modern vehicles for example, use computer and communication systems that provide essential functions like engine performance and safety sensors [2]. Modern buildings use connectivity to control functions like heating, venting, air conditioning, security, lighting, etc. [2].

Some of the most common household IoT devices include voice and app-controlled devices such as Amazon Echo and Google Home. These devices are used for home automation that enable the user to effortlessly complete simple tasks such as turning on lights, ordering food, setting a timer, etc. The technology of IoT certainly makes daily life easier for individuals, but its real utility and significance exists in its uses for the broader society, such as industrial and infrastructural functions, like monitoring power grids and sending important information to utility workers [6]. Entire cities can use IoT to improve lives by measuring certain things such as air quality, traffic control, and increase small conveniences such as monitoring available parking spaces in a public area [6]. The applications range far and wide in society, ranging from smart home appliances to smart agriculture. The uses of IoT are not limited to a particular industry or function; it is only limited by the imagination.

One of the most impactful applications of IoT is in healthcare. IoT in healthcare is extremely important because it directly improves the quality of life of patients. The ways in which IoT can be applied in the medical field alone is growing exponentially. Smart pill boxes can detect how many pills are left and send reminders to their smart phone, a glucometer can detect glucose levels and send the information to an insulin pump to automatically dispense insulin, a monitor can be sent home with a patient to measure heart rate, blood pressure, oxygen levels, etc. Patient information can be collected and sent to healthcare provider who can review it remotely and make decisions from looking at the biometric data.

IoT is also emerging as an extremely lucrative field. Indeed, according to Von See, [7] the global IoT market was worth an astonishing $389 billion in 2020 and is expected to grow over one trillion USD in 2030. The consumer market holds the highest share at thirty-five percent [7]. Consumer IoT goods like smart watches, smart phones, smart appliances, and more recently, smart cars, top the charts in IoT development [7]. This number is also expected to grow to forty-five percent by 2030, and the total number of IoT devices globally is expected to triple in this time [7].

1.3 The Elements of IoT

A device, system, or application considered has a few things that make it specifically a part of the IoT environment. All IoT devices communicate with other devices or objects a part of the IoT environment where they send and receive information, process it, and present it through a program or application.

The basic building blocks of IoT include sensors that gather information about the environment, networks and gateways for information transmission, middleware which allows the components in the IoT devices to “talk” to each other when they otherwise would not be able to, a data processing and storage mechanism (e.g., the cloud), and finally a user interface which allows an end user to review the information [5]. These building blocks make up an IoT platform, but vary wildly in their implementation, purpose, and scope (i.e., IoT is heterogenous). Figure 1.2 below illustrates the key aspects of an IoT system.

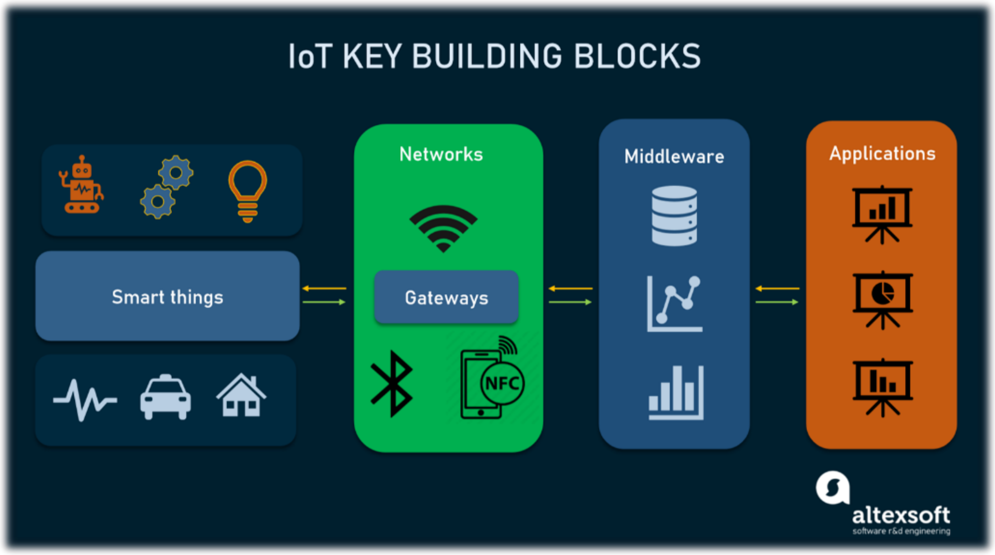


Figure 1.2: IoT Key Building Blocks [8]

While those are some of the basic building blocks, Burhan, et al., [9] provide additional elements of IoT. These elements are identification, computation, services, and semantics. Each IoT object must be able to identify in the IoT system through naming and addressing processes [9]. An example of a naming process is using electronic product codes, whereas an addressing scheme is completed through IPv4 or IPv6 which provides a unique address [9]. More than one device may share a name, but each device has its own unique address [9].

For the computation element, the information gathered from IoT devices is filtered by some computational means, removing superfluous or irrelevant data [9]. For IoT software, the operating system (OS) plays a significant role in computation [9]. The services element refers to the services provided by the IoT application [9]. There are four service types: identity service, information aggregation, collaborative service, and ubiquitous service [9].

Identity service refers to the identity request sent by IoT objects [9]. There are two types of identification: active and passive [10]. Active identification process relies on a continuously powered device (e.g., battery powered) that broadcasts information [10]. Passive identification is powerless and relies on an external reader and electromagnetic field to gather information, such as a powerless RFID tag that requires a reader in order to transmit data [10]. Information aggregation collects and process all the information gathered and transmits it to the application [9]. The collaborative service makes decisions based on the information aggregated and sends the response to the IoT devices [9]. Finally, the ubiquitous service executes the response command immediately and seamlessly in the IoT system [9]. Semantics in IoT generally refers to the interoperability of IoT systems while automatically providing clear meaning of the data [11]. Figure 1.3 below illustrates the elements and cycle of an IoT system.

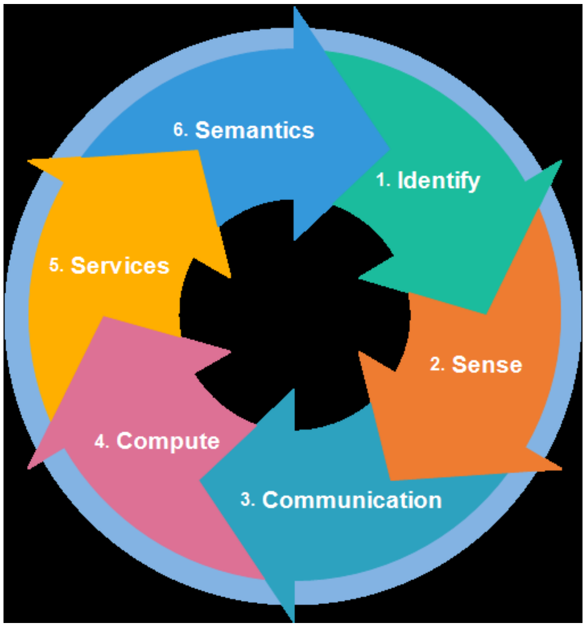


Figure 1.3: Elements of an IoT System [9]

While the foundational aspects of one IoT system remains similar to others, it varies with its application. For example, an IoT system that is implemented for more efficient farming by timing irrigation using sensors to detect moisture levels will have a different architecture and function differently than an IoT system implemented for sensing biometric data in a patient, such as blood sugar levels, and automatically dispensing insulin through an insulin pump. While the IoT agricultural system may use simple sensors such as radio frequency identification tags to detect soil pH and moisture and send that information through an RFID reader, the biometric IoT system may use an implant sensor for blood sugar sensing, a pressure cuff with an embedded sensor for blood pressure, and a weight scale with Bluetooth capability that uses an entirely different suite of protocols from the agricultural system.

Additionally, those that collect the data may do so in a variety of ways. The agriculturist may use a local data processing and storage system to collect and view the information, whereas the healthcare provider may utilize cloud services to process and store the electronic protected health information (ePHI). So, while the function is similar (sensing the environment, processing/ storing, and viewing the data), the method in which the entire IoT system operates is vastly different.

This is the heterogeneity of IoT; different components, hardware, software, protocols, tools, and services utilized in the entire process depending on its purpose. While this is not necessarily a negative thing, it is important to recognize that it does lead to challenges within the IoT environment regarding cybersecurity, standardization, and efficiency. It becomes more tedious and difficult to apply security practices that sufficiently protect different devices, suites of protocols, and applications. For example, the same encryption method for data cannot be applied to every IoT system. Bluetooth encryption methods may vary from encryption that cellular networks or WiFi use.

In addition, the efficiency and goal of the IoT system is important for determining what type of IoT components to use. Going back to the agriculture example, an extremely low power device that uses simple protocols may not be able to manage the substantial amounts of data gathered from acres upon acres of farmland and may lack the processing power for any encryption methods. There are numerous aspects of the IoT system to consider for users. Is security more important than efficiency for its purpose? Is it important that the device has a powerful battery and long battery life? Is it necessary to use a flexible and scalable storage system like the cloud? These are just a few basic questions that scratch the surface of IoT capability.

Chapter 2: The Architecture of IoT

This chapter explains the specific architecture of IoT systems: all the layers of IoT and how they operate. The building blocks of IoT systems are expanded upon and illustrated. The details of specific communication systems, such as Wireless Sensor Networks (WSNs), Wireless Personal Area Networks (WPANs), and Wireless Body Area Networks (WBANs) are discussed. These wireless systems vary in architecture and function but are all considered systems of IoT. A brief overview of cloud services for IoT is discussed, and finally some general challenges to IoT are presented.

2.1 The Structure and Layers of IoT

The elements of IoT were previously discussed, so understanding how those elements work to build the structure and architecture of IoT is necessary. It is worth noting that there is not a single standard architecture of IoT, rather there are many designs of IoT architecture that fit the purpose. Like the Open Systems Interconnection (OSI) model in a networking system, IoT has conceptual architectures that function similarly. The most common architectures are the three-layer, service-oriented, and five-layer models [3].

The three-layer model consists of three essential layers: the perception layer, the network layer, and the application layer [3]. The perception layer is also referred to as the physical layer because this contains the tangible devices and sensors embedded within that allow the architecture to exist [3]. The physical sensors or devices that gather the information about the environments are a part of the perception layer. They interact with the environment around them and have computing power that make them “smart” [12].

The network layer is responsible for communication between the physical devices, sending and receiving information collected through either a wired or wireless connection to the application layer [3]. This layer transports the information gathered from the perception layer through certain protocols [12]. There are a vast number of protocols and communication technologies that IoT uses, so it is important to consider the efficiency and security before deployment. The application layer provides the applications and services of the IoT system [3]. The functionality of IoT is performed in the application layer [12]. Data processing, analyzing, and presentation occurs in this layer [12]. The data from previous layers is made available to the actual application running the IoT device (e.g., the smart car) [12]. Figure 2.1 below illustrates the three- layer IoT architecture.

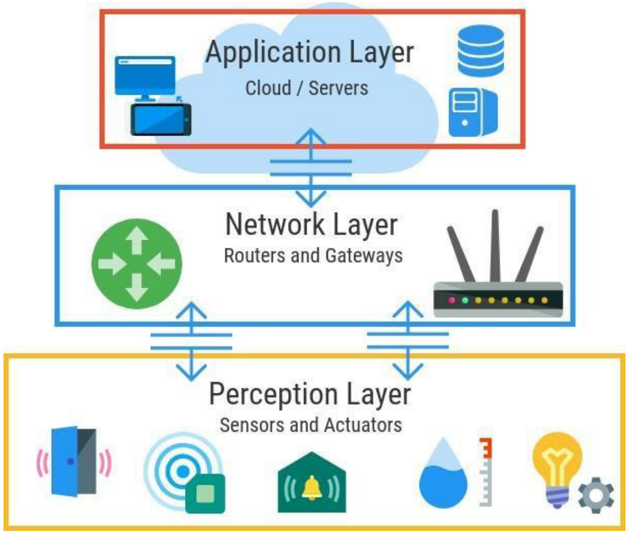


Figure 2.1: Three-layer IoT Architecture [13]

The service-oriented architecture (SoA) has the same three layers with a service layer between the network and application layer. This architecture revolves around the services of IoT applications and provides service discovery, service composition, service management, and service interfaces in the service layer [12]. The SoA provides dynamic data retrieval and service discovery, the process of locating service requests in an efficient manner [12]. Service composition is used for connecting the devices and getting the requests [12]. Service management manages the requests and interprets them [12]. Service interfaces allows for interoperability between services [12].

The SoA is popular in enterprise systems because of its cost-effectiveness and the reusability of hardware and software [5]. The service layer also provides application programming interfaces (APIs) that provide the service interface to end users, i.e., how people see and interact with the data [5]. Figure 2.2 below shows an example of an SoA.

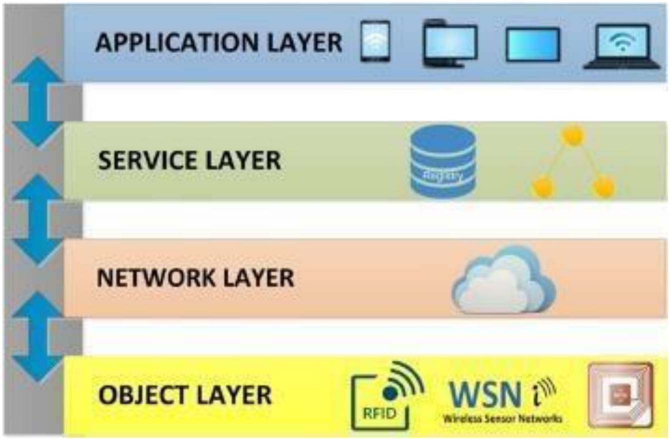


Figure 2.2: Service-oriented Architecture [13]

The five-layer architecture consists of the three-layers from the three-layer model, with additional layers of the middleware layer between the network and application layers, and the business layer on top of the application layer. The middleware layer is especially important for a large IoT environment that contains multiple different communication technologies. The middleware layer is responsible for taking all the information gathered from IoT devices that use different communication methods and with it, different suites of protocols (e.g., Bluetooth and ZigBee) [12].

Middleware is software or a service that formats and processes the information sent through a gateway for the application to understand the vast amount of data coming through from various IoT sources [12]. Essentially, middleware bridges the gap between the network and application layers and allows the different technologies in IoT to be compatible with one another. The business layer is relatively straightforward, it is the layer for retrieving and managing data to assist with business management [14]. The data from IoT concerns business goals and is useful for answering important questions, so the business layer refers to the usefulness and analysis of the data [14]. Figure 2.3 illustrates the five-layer model.

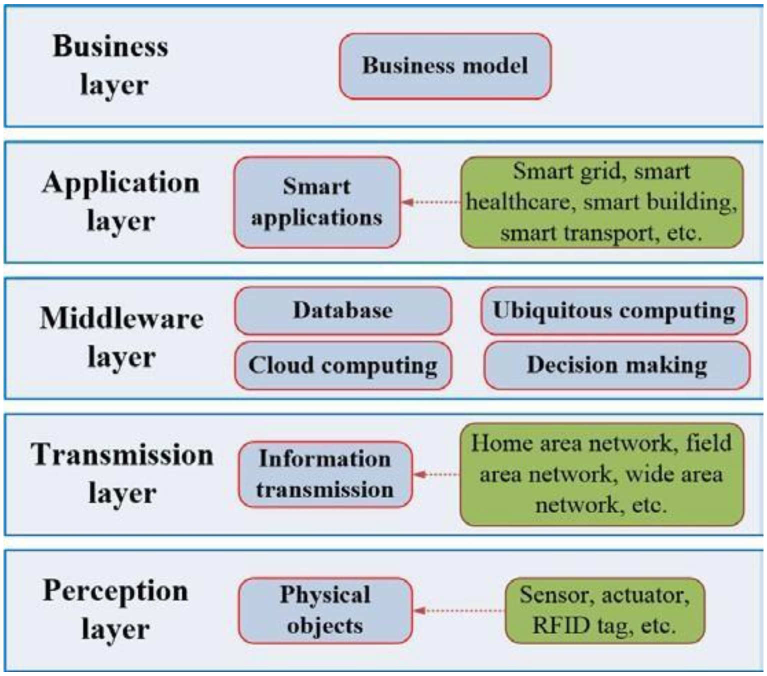


Figure 2.3: The Five-Layer IoT Architecture [15]

These models are the most common models of IoT. There are numerous architectures of IoT, as each one can be implemented to fit the needs of the business or organization. IoT is an extremely flexible networking system that provides practical functionality in virtually any field for any purpose. The heterogeneity of IoT architecture introduces standardization and communication challenges, leading to the further development of technology such as middleware.

2.2 Key Technologies of IoT

Wireless sensor networks (WSNs) are a key technology of IoT. WSNs are the foundation for IoT, interconnected sensors sending and receiving information. WSNs are lossy networks that provide wireless communication between small sensors, referred to as nodes, which connect to a central node or gateway to route the traffic to the internet [16]. WSNs are implemented for large scale event and environment monitoring. The WSN architecture consists of sensor nodes, gateway, and the user [16]. WSNs typically consist of low-power and resource constrained devices that serve a simple purpose, such as sensing temperature and forwarding that information through the gateway. A simple WSN model is illustrated in Figure 2.4 below.

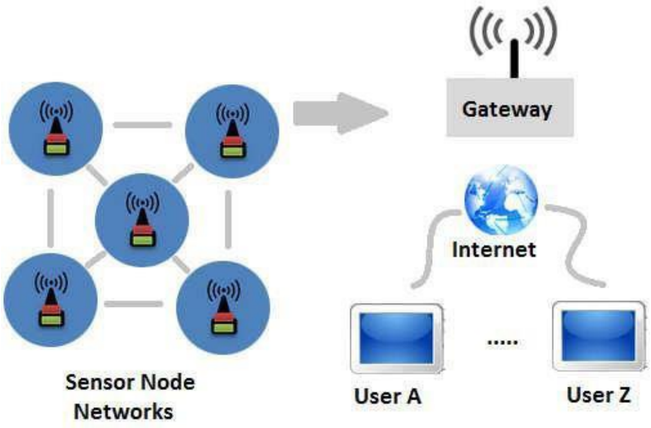


Figure 2.4: WSN Model [16]

The sensor nodes of a WSN usually have a limited broadcast range, so the placement of the nodes is important for sensing and retrieving accurate data. The nodes of a WSN can use different network topologies, such as linear, star, or mesh [16]. Even though the sensor node is resource constrained, it still has sufficient processing and computing power [16]. The sensor nodes must also have a power source, this is usually through battery power, although they can be powered with means such as solar or thermoelectric [16]. The sensors spend most of the time in a hibernation state, only waking up and consuming power when they are actively collecting, sending, or receiving information [16]. WSNs use communication methods like Bluetooth, ZigBee, and 6LoWPAN, which will be discussed in-depth later.

WPANs, a similar communication system to WSNs, take the interconnectedness of sensors spanning a distance, and shorten it to the environment of the human personal space [17]. WPANs often use the same protocols as WSNs – Bluetooth, ZigBee, etc. Some of the common devices that make up WPANs are laptops, smartphones, headphones/earbuds, speakers, printers,etc. WPANs encapsulate all the wireless technology around an individual or space. WPANs are flexible and low cost but provide lower coverage and data rates [17]. Figure 2.5 below illustrates aWPAN environment.

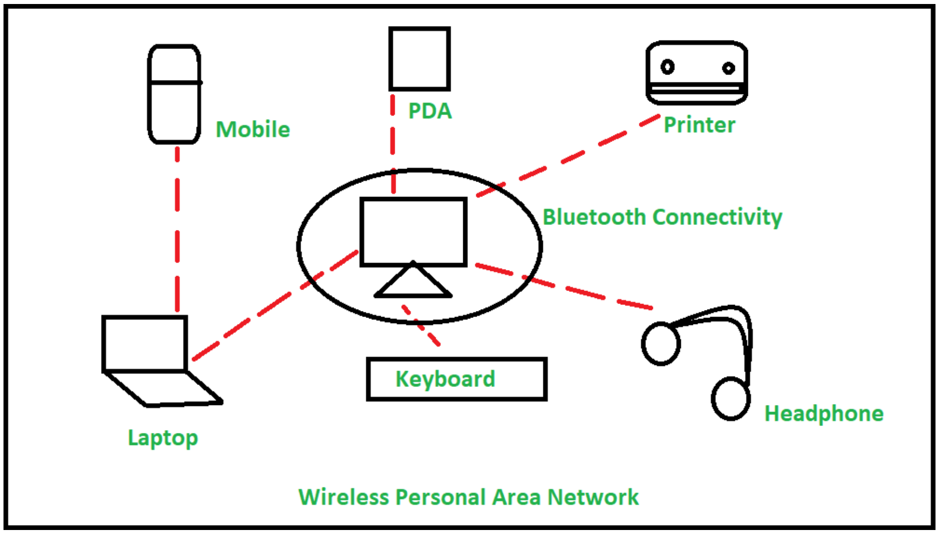


Figure 2.5: WPAN Environment [18]

WBANs are like WPANs but monitor conditions in or directly around the human body [19]. WBANs are most implemented for medical purposes, like implants or wearable devices to sense and record biometric data, but its applications also extend beyond the medical field. WBANs can be applied to athletes to measure heart rate, temperature, respiration rate, etc. to analyze the data and improve performance to gain a competitive edge and increase fitness. WBANs are crucial for the evolution of healthcare and an integral part of IoT for patient monitoring. Some common consumer WBAN devices are wearables such as Fitbit and other smart watches, namely Apple Watch and Samsung watches. Figure 2.6 below illustrates the WBAN environment.

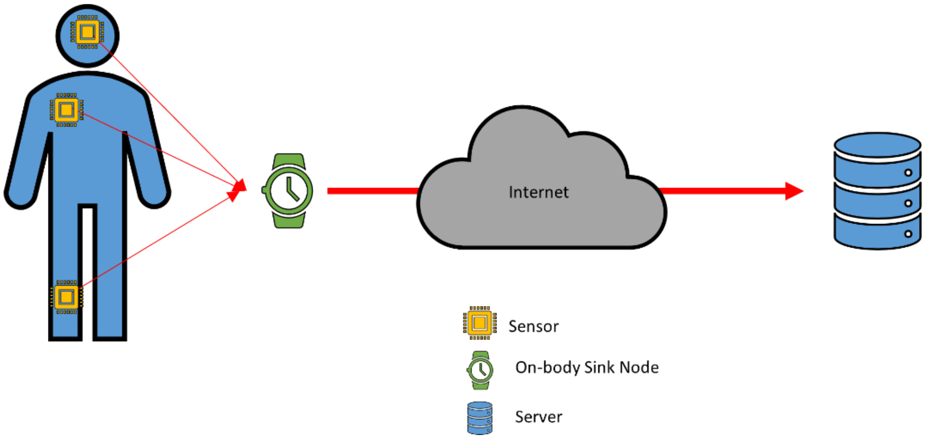


Figure 2.6: WBAN Environment [19]

WSNs, WPANs, and WBANs are interchangeable communication systems that use similar protocols. They can all be implemented in a variety of ways for a variety of purposes and are critical to IoT functionality. They remain flexible, low-power, and low-cost options for sensing and wireless communications. While they can be implemented in several ways, there are challenges such as low fault tolerance, security vulnerabilities, and channel interference. These will be discussed in-depth further. Currently, one of the necessary and growing tools in IoT for data processing, security, storing, and management is the cloud.

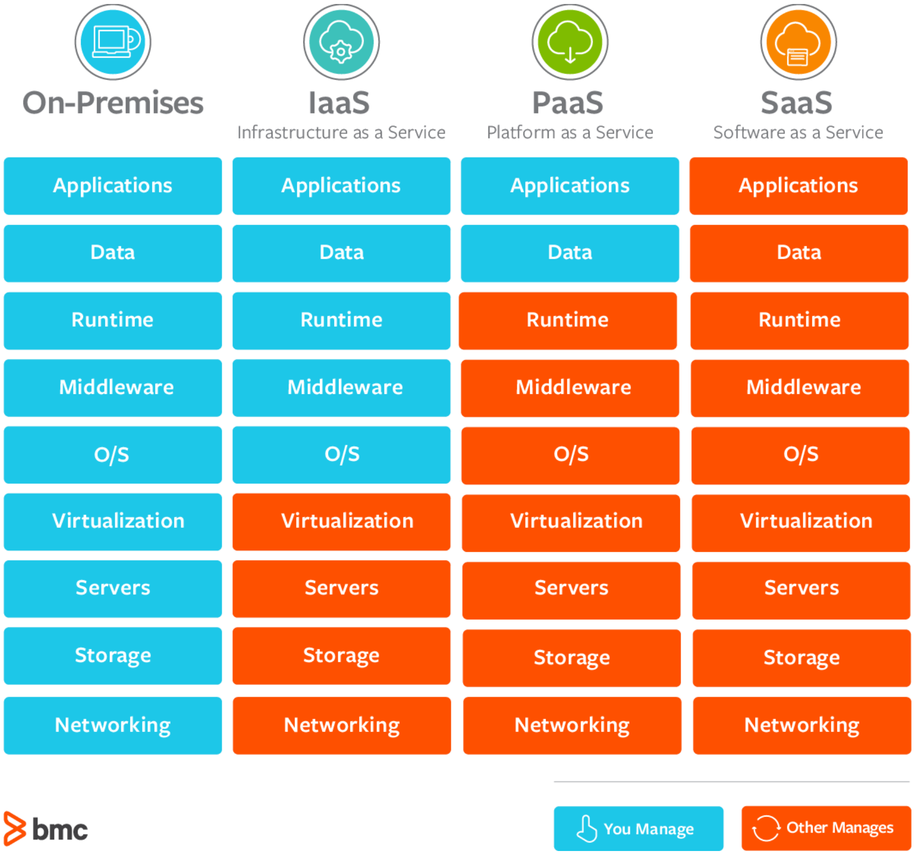
2.3 Overview of Cloud Computing and IoT Services in the Cloud

The cloud is a large network of servers that provide services for anyone that needs it. The cloud is a flexible, scalable platform that offers many services and solutions to modern IT environments. The cloud can be used for data storage, streaming services, application development, and plenty more. The cloud works by outsourcing physical equipment, such as servers, from a local environment to a cloud provider, notable ones being Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

The cloud providers have access to a large network of servers across the globe that can be accessed by anyone who needs the service. Most cloud providers use a pay-as-you go model, charging by usage, so an organization that cannot afford the network infrastructure and maintenance on-site may choose to use a cloud service and pay for services by usage. There are three primary service categories that the cloud offers: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

IaaS allows access to servers, storage, and general networking infrastructure that users can configure. The cloud provider manages all the hardware. IaaS is beneficial for reducing costs in an on-site IT environment where resources can be scaled up and down depending on need.

PaaS provides users with the means to develop and run applications. The cloud provider manages most of the resources in PaaS, including the software, operating system, middleware, etc. PaaS is mostly beneficial to application developers who can easily build, test, and run applications in the PaaS. SaaS is the most popular and widely used cloud service option. SaaS is completely managed and operated by the cloud provider and the end user can access the software on any internet-connected device. SaaS is beneficial for streaming and subscription services, some of the most popular being Amazon Prime, Netflix, and Spotify. Figure 2.7 illustrates the differences between on-premises, IaaS, PaaS, and SaaS.



On-Premises	IaaS Infrastructure as a Service	PaaS Platform as a Service	SaaS Software as a Service
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Figure 2.7: On-Premises, IaaS, PaaS, and SaaS [20]

The cloud can be used for many different services, one of those being IoT. Since an IoT environment collects an enormous amount of data from information aggregation, the cloud has become a popular and convenient service for IoT. The cloud is commonly used for big data storage and providing applications for IoT devices. All three services can be used for IoT systems and provide effective services. IaaS can be used for big data storage and scale the needs for IoT. PaaS can be used for IoT application development and application programming interfaces. SaaS can be used to quickly access software relevant to the IoT device.

An IoT environment is not required to use the cloud, but the cloud makes an IoT system much more effective. For example, data gathered from a smart farm in one location of the U.S. can be compared to data gathered from another location in the U.S. to draw insights to improve agriculture development. The information collected from sensors in smart farms, such as soil, pH, temperature, humidity, etc., can be stored in the cloud and provide access to users.

Without the cloud storage, being able to compare and access the data of the different locations would be extremely difficult. The cloud improves the efficiency of IoT, which ultimately improves the lives of many. The storage can also be scalable, upgrading the needs of storage if more sensors are placed or more smart farms are added as IoT environments. Cloud storage also shifts the burden of storage from the resource constrained devices to the cloud. As briefly mentioned earlier, IoT devices are often low-power, low-activity devices that cannot afford to expend much energy beyond their direct purpose. This mostly concerns the sensing devices in an IoT environment that use simple communication protocols rather than resource heavy TCP/IP communication. While the cloud is a powerful tool for IoT, it does not solve every problem with it.

2.4 Key Challenges in IoT

Some challenges in IoT have been mentioned previously, such as heterogeneity – the diversity of devices and protocols that limit interoperability. Security, privacy, ownership of information, encryption, access control, authorization, authentication, and lack of standardizations are all challenges an IoT environment faces. Confidentiality, integrity, and availability are the core tenets of cybersecurity in computer and network systems. The same is true for IoT systems.

Confidentiality ensures that all information and data remain confidential; that only the trusted devices and parties are able to access and view information. Integrity refers to the accuracy of the information. It is important that all information in an IT environment remains unaltered and unaffected; the information that was sent needs to be the same information that is received. If any information from point A to point B is altered or lost, there was a lack of integrity. Availability refers to the accessibility of information. The information needs to be accessible by authorized parties at any point in time. This also encompasses data backup and recovery, if information is somehow lost, there needs to be methods in place to retrieve it.

It is necessary for all devices and components in IoT to be able to communicate quickly and effectively with one another, but it is also necessary that the communication between devices is trusted and verified, i.e., the device must be who it says it is. A device not a part of the IoT environment that can monitor the traffic between IoT devices or even connect itself between communications as a trusted device is a major concern. This is known as a man-in-the- middle (MITM) attack and if IoT security is not sufficient, a bad actor could effortlessly see all the transmission data between devices. An external device being able to view the transmission data already violates confidentiality of the IoT environment. The data could be stolen and held for ransom, known as ransomware. Some of the most concerning security threats in IoT are MITM attacks, ransomware, Denial of service (DoS) attacks, and phishing.

The heterogeneric nature of IoT can make it difficult to choose an efficient architecture and implementation method. While middleware helps standardize communication and data transfer, the devices must be compatible in the environment. For example, simple sensors detecting temperature must be able to transmit that information over some protocol to another device or gateway, which must be able to receive and transmit the data without altering it. The 'language barrier' of IoT can be an issue in some cases.

There is also the challenge of encryption. The data that is transmitted in the IoT environment should have encryption methods to protect the data at rest and in transit. The main issue with encryption is that it can potentially consume a lot of power and resources from the IoT devices, if they are even capable of encryption [21]. In the healthcare sector, encryption is paramount because of the sensitivity of data being recorded and transmitted. In healthcare, extremely personal data is being collected and sent over communication channels. Personal data such as heart rate, weight, blood pressure, blood oxygen levels, glucose levels, etc. can be all collected by internet of medical things (IoMT) devices. It is important to ensure secure transmission because of compliance regulations such as HIPAA. These challenges will be addressed in-depth with the analysis of the LifeWatch Mobile Cardiac Telemetry 3 Lead device and the remote patient monitoring system of Vivify Health.

Chapter 3: The Purpose of IoT in Healthcare

This chapter introduces IoMT uses and applications for healthcare. IoMT can be used to provide quality care remotely which eases the burden of healthcare facilities and staff. Patients can receive quality care while in the comfort and freedom of their homes and communities. IoT is also beneficial for in-patient care, since many tasks that would require physical intervention (e.g., gathering vital signs) can be automated. The purpose of IoMT is to make patient care simpler and more efficient for the people involved.

3.1 Monitoring Patient Data to Enhance Quality of Care

Since IoT is a collection of sensors to monitor the environment, the environment can include human physiology. Physiological readings – also referred to as biometric data – can be sensed, recorded, and transmitted through IoMT devices for the purposes of patient care. According to Nausheen, et al. [22], there are three categories of IoMT applications: clinical care, remote monitoring, and context awareness. IoMT in clinical care refers to patients who are in intensive care units and require on-going monitoring to provide information to clinical staff about the progress of their condition [22].

In certain cases, it is more beneficial for a patient to be monitored with IoMT devices remotely from their home. Remote patient monitoring (RPM) allows hospitals and other healthcare facilities to make the decision of admitting patients or sending them home to use RPM for further monitoring if it is safe to do so. Thus, freeing up a room for a future patient who may require inpatient care while still providing service and care to the remote patient. This application commonly used for patients with chronic conditions or diseases [22]. Context awareness refers to gathering information about a patient and their environment and understanding the affect an environment may have to a patient's circumstances [22]. For example, a smart device could detect low air quality in a patient's environment and send alerts to a healthcare provider if the air quality is affecting the patient's respiration.

There are also different ways to monitor patients. IoMT devices include sensors that attach to the human body but can also include wearables and implantable devices. Wearables are devices that a patient can wear, such as a watch, that is integrated with IoMT. An implantable device is a device that can be inserted into the human body. An example of an implantable device is a pacemaker. Pacemakers can now be integrated with the IoMT environment to provide instant information about a patient's cardiac rhythm and overall heart health.

The vulnerable population, i.e., children, the elderly, and those with chronic conditions benefit the most from IoMT and specifically remote monitoring. RPM also provides a personalized treatment plan that encourages patient/doctor interaction [22]. RPM also allows healthcare providers to know if a patient is following their treatment plan and regimen, whereas without IoMT the healthcare provider would have to take the patient's word for it until their next appointment or check-up. With IoMT, the quality of care is drastically enhanced from traditional healthcare. Patients now have flexible options to continue treatment outside of the healthcare facility. IoMT also allows the patient to signal an emergency and immediately notify healthcare providers and emergency services [22].

3.2 Efficiency of IoMT for Healthcare Providers

While IoMT helps patients receive quality care, IoMT can also be a powerful tool for healthcare providers. IoMT can help with diagnosing conditions through real-time monitoring. Continuous monitoring of a patient's physiology can provide healthcare professionals with great insight into a person's health beyond what would have previously been possible. IoMT eases the burden of healthcare workers by outsourcing treatment to RPM. It also relieves healthcare staff for in-patient monitoring by reducing the workload. An IoMT device automatically sensing and sending biometric data of a patient reduces the need for physical or manual intervention, allowing healthcare staff to focus on other aspects of their work.

IoMT also allows for easier and quicker access to data. Electronic health records (EHR) are simpler to access with mobile apps. Mobile apps assist healthcare providers with precise assessments, examinations, and diagnosing of patients [22]. It is no longer necessary for healthcare professionals to keep track of physical bulky patient charts, all patient data can now be stored and accessed through mobile apps. IoMT apps can also assist healthcare providers with providing electronic educational information about conditions and treatments options [22]. A medical reference guide can be in the application that healthcare providers use, providing quick resources and information to healthcare professionals that may need it [22]. Additionally, IoMT is cost-effective for healthcare providers as well. Leaning on IoMT resources reduces healthcare costs for the healthcare business [22].

3.3 Other Applications of IoT in Healthcare

There are other uses of IoT in healthcare that provide services other than direct medical care. One example is wheelchair management [22]. Yang, et al. [23] propose a method for integrating wheelchairs with IoT to assist people with disabilities and limited movement. By enabling IoT capabilities on wheelchairs, there can be a closer watch on the vulnerable population to reduce harm. A wheelchair can be equipped with sensors that can detect if an individual falls out of the wheelchair or if the wheelchair rolls over [23]. The pressure sensors in the wheelchair intelligently detect the wheelchair's position and the person's movement [23]. The collection of sensors can communicate through a gateway, such as a smart phone, and send distress signals for medical assistance [23].

An additional application of IoMT includes medication management. As Yang, et al. [24], have proposed, a medication delivery system integrated with IoT enables real-time tracking of medication called the iMedBox. The iMedBox is a medication box enabled with RFID tags, WiFi, and WBSNs to track medication inventory, send reminders to patients, and record all activity such as missing a dose and throwing away/destroying medication [24]. The iMedBox is one prototype that could help patients with their medication tracking and relieve medication non-compliance, i.e., patients mismanaging and improperly handling medication.

Some major concerns regarding the applications of IoMT include security, privacy, and compliance. IoT security is a major concern for hospitals and medical care facilities. The healthcare sector has the highest number of breaches [25]. Indeed, from 2015 to 2019 the healthcare sector accounted for 76% of all breaches, well above the other sectors, with the business and financial sector accounting for 9% [25].

The applications of IoMT are numerous. So long as there is interoperability, reliability, a sufficient level of security and compliance, then IoMT will revolutionize the healthcare system and reduce the burden of patient care on healthcare staff and shift that burden to technology. Interoperability and reliability are contingent upon the architecture and mainly the communication protocols of IoT. The heterogeneity of IoT does produce challenges with IoMT implementation but understanding how the protocols operate is crucial to a successful IoMT deployment.

Chapter 4. The Protocols and Technologies of IoT

This chapter discusses some key protocols and technologies of IoT, how Bluetooth operates and some of its major vulnerabilities, how IoT uses cellular network technologies such as LTE, and how IoT requires lightweight encryption methods. The nuts and bolts of IoT are the protocols that allows communication. Protocols are what makes IoT an intelligent operation. Understanding the protocols is necessary to understand how to secure them. Security is a necessary component of IoMT, so the vulnerabilities of technology such as Bluetooth is important to understand. An overview of cellular technology is introduced, and lightweight encryption methods are proposed.

4.1 Overview of Key Protocols: RFID, CoAP, MQTT, XMPP, AMQP, 6LoWPan

There are many protocols in IoT that have been developed to perform certain functions and meet certain needs. The precursor to modern IoT protocols is RFID technology. Babu, et al. [1], provides a detailed explanation: the way RFID works is an object is tagged with a chip that provides the information about that object, which an RFID reader sends a query signal to. The tag receives the signal and sends a reflection signal back to the reader. The transmission exchange is sent to a database which confirms the identity of the object. RFID technology is considered the first machine-to-machine (M2M) communication technology [1]. While RFIDs are still useful, IoT has progressed to use more advanced protocols.

One of the key protocols in the application layer of IoT architecture is the constrained application protocol (CoAP). CoAP utilizes Representational State Transfer (REST) to provide functionality through hyper-text transfer protocol (HTTP). REST is an architecture that provides simple exchanges between client and server over HTTP using GET, POST, PUT, and DELETE request methods [1]. HTTP is a request/response communication protocol widely used on the internet and is often too dense and power consuming for IoT [26]. CoAP was designed by the Internet Engineering Task Force (IETF) Constrained RESTful Environments group (CoRE) to provide lighter HTTP functionality [1]. CoAP essentially uses the HTTP request/response method and shrinks it into a usable format for IoT.

A core difference between HTTP and CoAP is that HTPP runs on transmission control protocol (TCP) while CoAP runs on user datagram protocol (UDP) [26]. TCP is a reliable protocol that establishes connections between sender and receiver. UDP is unreliable and does not establish connections between sender and receiver. The sender and receiver in TCP both establish that a connection is occurring before data is transmitted and closes the connection, guaranteeing the data will be sent and received.

In UDP, the connection is not established before data is transmitted, meaning that a packet may not reach its destination. For this reason, UDP is considered unreliable. Although TCP is reliable, it is slower than UDP because of the handshake process, i.e., confirming and closing the connection. UDP also enables broadcast and multicast functionality. Broadcast communication sends signals to all devices on the network and multicast sends signals to specific multiple receivers. For these reasons, UDP is effective in IoT because ofthe simpler and lightweight communication. Thus, CoAP is an efficient protocol that adapts HTTP methods and reduces HTTP to a smaller size. Figure 4.1 below illustrates the TCP and UDP processes and Figure 4.2 illustrates the CoAP architecture.

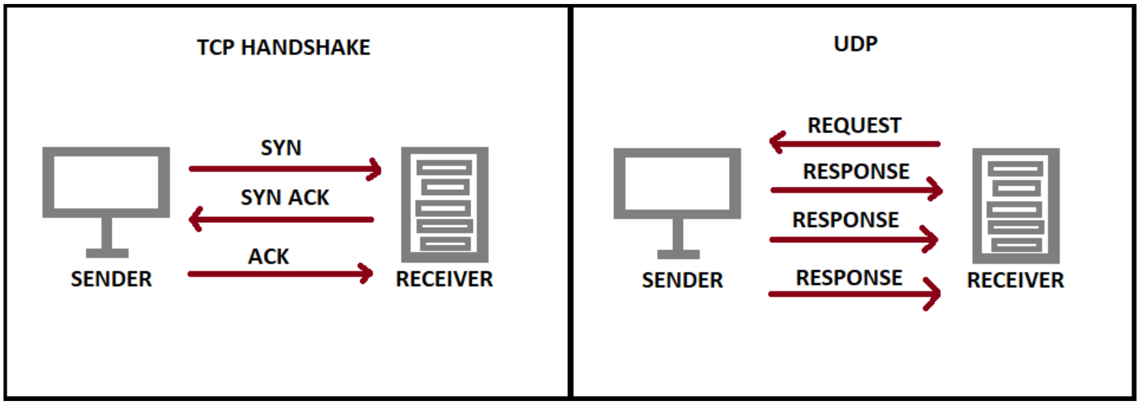


Figure 4.1: TCP Handshake Process vs UDP [27]

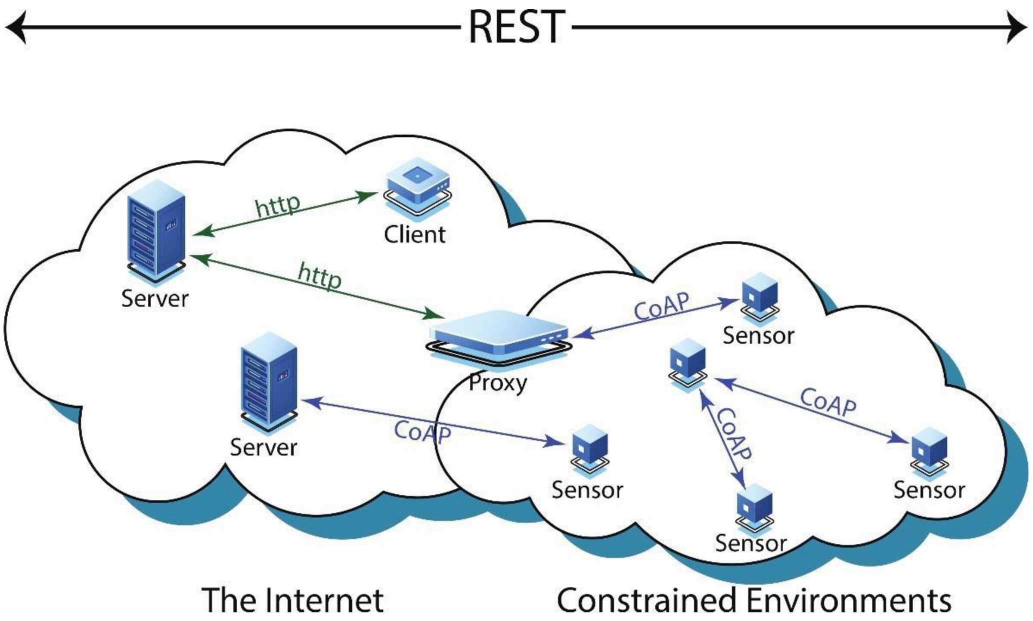


Figure 4.2: CoAP Architecture [28]

Another key protocol for IoT is message queue telemetry transport (MQTT). MQTT is another protocol like CoAP, but a key difference is that it runs on TCP/IP rather than UDP. While CoAP is based on a sender/receiver model, MQTT uses a publisher/subscriber model [26]. A publisher/subscriber model differs from a sender/receiver model by the fact that there is no direct connection between the publisher and the subscriber [26]. There is no handshake process, rather the publisher and subscriber communicate through a broker who broadcasts messages to all possible subscribers of a topic [26]. MQTT is a lightweight protocol for IoT that ensures reliability through quality-of-service levels [26]. Figure 4.3 illustrates the MQTT publisher/subscriber model.

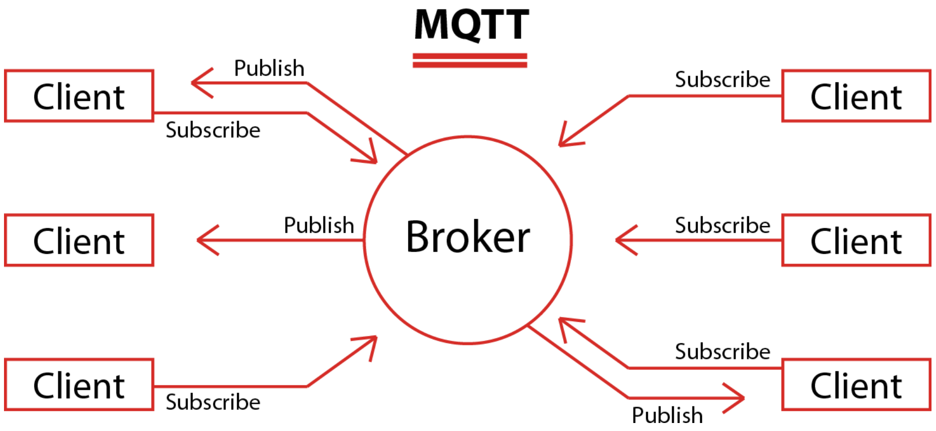


Figure 4.3: MQTT Publisher/Subscriber Model [29]

Advanced Message Queuing Protocol (AMQP) is another message-based application layer protocol that can use either the request/response or publish/subscribe models [26]. AMQP runs on TCP [26]. Because of its security and reliability, AMQP is used in corporate environments [26]. AMQP uses a messaging queue to provide efficient communication [26]. Another notable application layer protocol is the Extensible Messaging and Presence Protocol (XMPP).

XMPP is decentralized and can be used with any operating system [1]. XMPP allows for telecommunication methods such as multi-party, voice, and video chatting [1]. XMPP differs from other protocols as it does not allow for machine-to-machine communication, but multiple XMPP servers acknowledge each other over the same network [26].

IPv6 over low power wireless personal area networks (6LowPAN) is a standard for low power and lossy networks (e.g., WSNs) [30]. IPv6 is a networking IP protocol that can be applied to IoT. 6LowPAN allows for complete IP-based wireless sensor networks. Every sensor or node in an IoT network has its own Ipv6 address and can connect directly to the internet creating a mesh network [30]. It uses AES-128 encryption at the link layer but relies on upper layers for end-to-end encryption [30].

These protocols and standards are key technologies for IoT. They are what allow IoT to function as an intelligent system of communication. Understanding the protocols and how they work helps with planning all aspects the IoT environment, especially security. There are many other protocols and standards of IoT, but these are common and notable. The variance in protocols is what makes interoperability difficult to achieve in an IoT environment. Ensuring each device can communicate with one another while remaining secure is paramount. One of the more common and ubiquitous standards for IoT is Bluetooth technology. Bluetooth is a part of almost every smart device and allows for effective communication. Bluetooth is integral to IoT as there are a plethora of implementations that utilize it.

4.2 Bluetooth Technology

Bluetooth is an open standard that communicates through short range radio frequency [31]. Bluetooth is used primarily for WPANs and ad hoc networks [31]. Bluetooth is prolific and exists in many consumer devices such as mice, keyboards, headsets, automobiles, printers, speakers, medical devices, etc. [31]. Bluetooth requires two or more devices to establish communication. Once the two (or more) devices are connected on the same channel and frequency through the pairing sequence, the formed network between them is called a piconet (tiny network) [31].

Bluetooth completely replaces cable connection by allowing wireless communication. For example, a headset would traditionally have to be wired to a PC, but with Bluetooth the headset can function wirelessly. Bluetooth also allows file sharing, synchronization, and internet connectivity between devices [31]. There are different versions of Bluetooth which range from the older version 1.0 to the current version 5.2. Every version of Bluetooth from 4.2 onwards is considered Bluetooth Low Energy (BLE) [30].

Bluetooth uses the 2.4000 gigahertz (GHz) to 2.4835GHz Industrial, Scientific, and Medical (ISM) frequency band [31]. Other standards use this band such as wireless local area networks (WLANs), so interference can be an issue. To curb this: “Bluetooth employs frequency hopping spread spectrum (FHSS) technology for transmissions. FHSS reduces interference and transmission errors but provides minimal transmission security” [31]. Bluetooth Basic Rate (BR) and Enhanced Data Rate (EDR) uses 79 different 1 megahertz (MHz) channels [31]. At each connection between devices, an available radio channel is selected by the FHSS process, and each device changes to the appropriate channel to allow communication. The channel is not used for long, and the channels repeatedly change to reduce interference and eavesdropping. This process is repeated until the devices disconnect.

BLE uses the same frequency band but uses 40 channels of 2 MHz width rather than 79 channels of 1 MHz width [31]. BLE also uses a time-division multiple access (TDMA) scheme to allow multiple users to share the same channel by dividing the transmissions into time slots, the sending device sending a packet at a predetermined time and the responding device responding after a predetermined interval [31]. This scheme allows for low energy performance. Bluetooth also utilizes a radio power measurement feature by automatically adjusting radio power based on signal strength [31]. This feature allows for Bluetooth devices to consume less power or stay within an agreeable range.

TDMA coupled with radio power measurement makes Bluetooth an excellent low-energy communication method. The key differences of BLE compared to Bluetooth BR/EDR are lower power consumption, lower memory needs, efficient communication methods, shorter packet lengths, and simpler protocols [31]. While BLE is an incredible technology, security is a major concern. There are also key differences between BR/EDR and BLE security features, mainly in the pairing and encryption methods. Since most IoT devices are low-energy devices, this thesis mainly explores the BLE security features and vulnerabilities. Table 4.1 below highlights the differences between BR/EDR and BLE. The security, pairing, and encryption methods are discussed in the following section.

Table 4.1: BR/EDR vs BLE [31]

<table>
<tr><th colspan="3">Characteristic</th><th colspan="4">Bluetooth BR/EDR</th><th colspan="3">Bluetooth Low Energy</th></tr>
<tr><td colspan="2">Prior to 4.1</td><td colspan="3">4.1 onwards</td><td colspan="3">Prior to 4.2</td><td colspan="2">4.2 onwards</td></tr>
<tr><td colspan="3">RF Physical Channels</td><td colspan="4">79 channels with 1 MHz channel spacing</td><td colspan="3">40 channels with 2 MHz channel spacing</td></tr>
<tr><td colspan="3">Discovery/Connect</td><td colspan="4">Inquiry/Paging</td><td colspan="3">Advertising</td></tr>
<tr><td colspan="3">Number of Piconet Slaves</td><td colspan="4">7 (active)/255 (total)</td><td colspan="3">Unlimited</td></tr>
<tr><td colspan="3">Device Address Privacy</td><td colspan="4">None</td><td colspan="3">Private device addressingavailable</td></tr>
<tr><td colspan="3">Max Data Rate</td><td colspan="4">1–3 Mbps</td><td colspan="3">1 Mbps via GFSK modulation</td></tr>
<tr><td>Pairing Algorithm</td><td colspan="3">Prior to 2.1: E21/E22/SAFER+</td><td colspan="2">P-256 Elliptic Curve, HMAC-SHA-256</td><td colspan="3">AES-128</td><td>P-256 EllipticCurve, AES- CMAC</td></tr>
<tr><td colspan="10">2.1-4.0: P-192 Elliptic Curve9, HMAC-SHA-256</td></tr>
<tr><td colspan="2">Device Authentication Algorithm</td><td colspan="3">E1/SAFER</td><td colspan="3">HMAC-SHA-256</td><td colspan="2">AES-CCM10</td></tr>
<tr><td colspan="2">Encryption Algorithm</td><td colspan="3">E0/SAFER+</td><td colspan="3">AES-CCM</td><td colspan="2">AES-CCM</td></tr>
<tr><td colspan="3">Typical Range</td><td colspan="4">30 m</td><td colspan="3">50 m</td></tr>
<tr><td colspan="3">Max Output Power</td><td colspan="4">100 mW (20 dBm)</td><td colspan="3">10 mW (10 dBm)11</td></tr>
</table>

4.3 Bluetooth Security and Vulnerabilities

Bluetooth has some built-in security standards for basic protection. There are five major security services built into Bluetooth: authentication, confidentiality, authorization, message integrity, and pairing/bonding [31]. BLE has four security modes each with additional levels in each security mode. The least secure mode is security mode 1 which does not offer authentication or encryption methods, while security mode 4 is the most secure as it offers both authentication and encryption. BLE can use several different pairing methods, the two main ones are legacy pairing and secure connection.

Legacy pairing works by key generation and distribution over a key transfer protocol. When pairing, the devices agree upon a temporary key (TK) whose value is determined by the pairing algorithm to begin the process [31]. A short-term key (STK) is then created based on the TK to encrypt the connection. The long-term key (LTK) – a key used for repeated encryption/ decryption – is then generated by one device and distributed to the other during pairing [31]. In addition to the LTK, other cryptographic keys such as the Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK) are also generated and distributed through a key transfer protocol [31].

The purpose of the IRK is to randomize the identity of a discoverable BLE device that can only be discovered by the trusted BLE device. Without IRK, the BLE device advertising itself as discoverable can be tracked by an adversary [31]. The CSRK is a key that authenticates the sender of the data and provides data signing, protecting information sent over unencrypted links [31]. Data signing is like a digital signature that proves it is the original and unaltered data, comparable to a human signature to verify documentation. Thus, CSRK provides authentication of the device and integrity of the data where the link is not encrypted [31]. Both keys are used to protect information from MITM attacks. However, the issue with the legacy pairing method is that unlike the pairing in the BR/EDR process, it does not use the Elliptic-Curve Duffie-Hellman (ECDH) cryptographic method [31]. ECDH is a secure cryptographic key agreement method that prevents MITM attacks and eavesdropping. Without ECDH, an LTK distribution in legacy pairing of BLE can be “overheard” by a third party.

Low energy secure connection is the other pairing method for BLE. Secure connection differs from legacy pairing in that it uses ECDH cryptography during pairing. The key generation is also different in that each BLE device generates its own LTK, rather than using the STK to generate the LTK and distribute it through a key transfer protocol. This method is more secure and provides protection against MITM attacks and eavesdropping by using ECDH cryptography and generating an LTK independently [31]. Once the LTK is generated on each device, the link is encrypted using the LTK and the IRK and CSRK are distributed [31]. Figures 4.4 and 4.5 on the next page illustrate the pairing process of BLE legacy pairing and secure connection pairing, respectively.

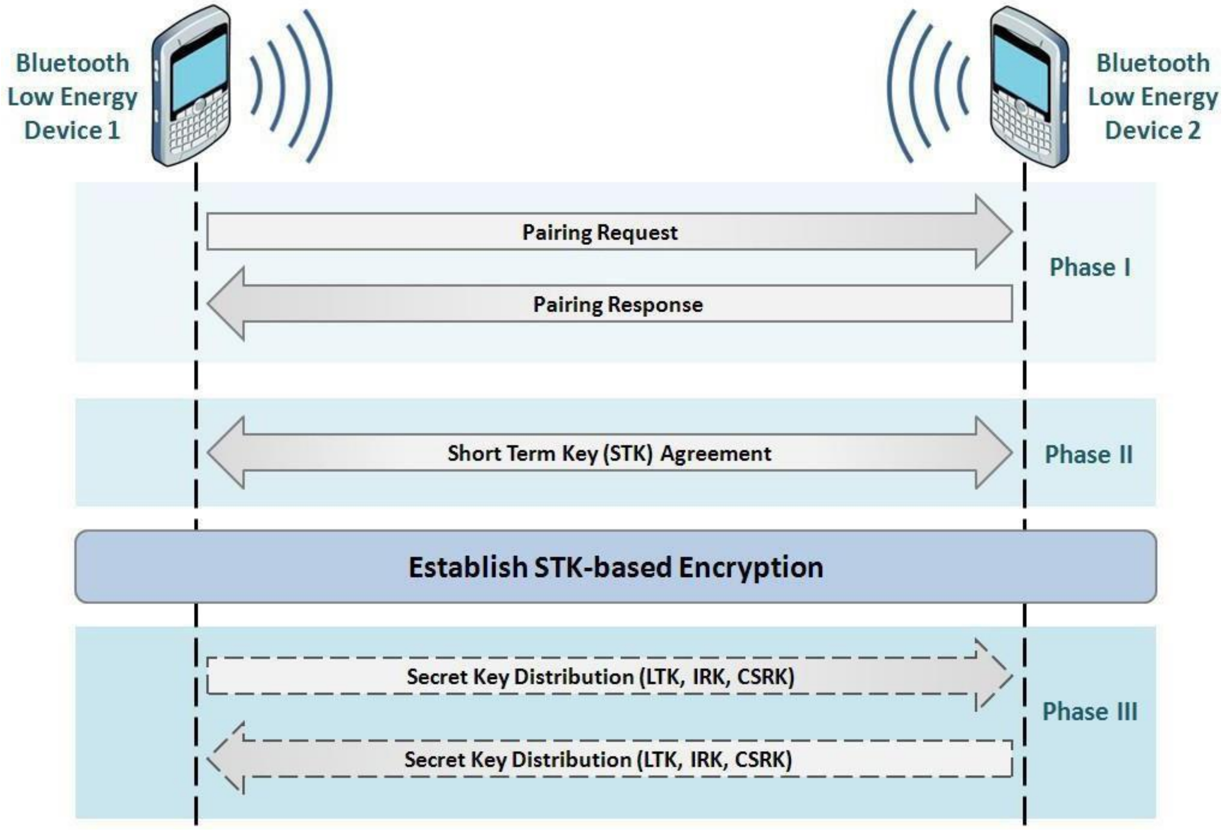

Bluetooth Low Energy Device 1
Bluetooth Low Energy Device 2
Pairing Request
Pairing Response
Phase I
Short Term Key (STK) Agreement
Phase II
Establish STK-based Encryption
Secret Key Distribution (LTK, IRK, CSRK)
Secret Key Distribution (LTK, IRK, CSRK)
Phase III

Figure 4.4: BLE Legacy Pairing [31]

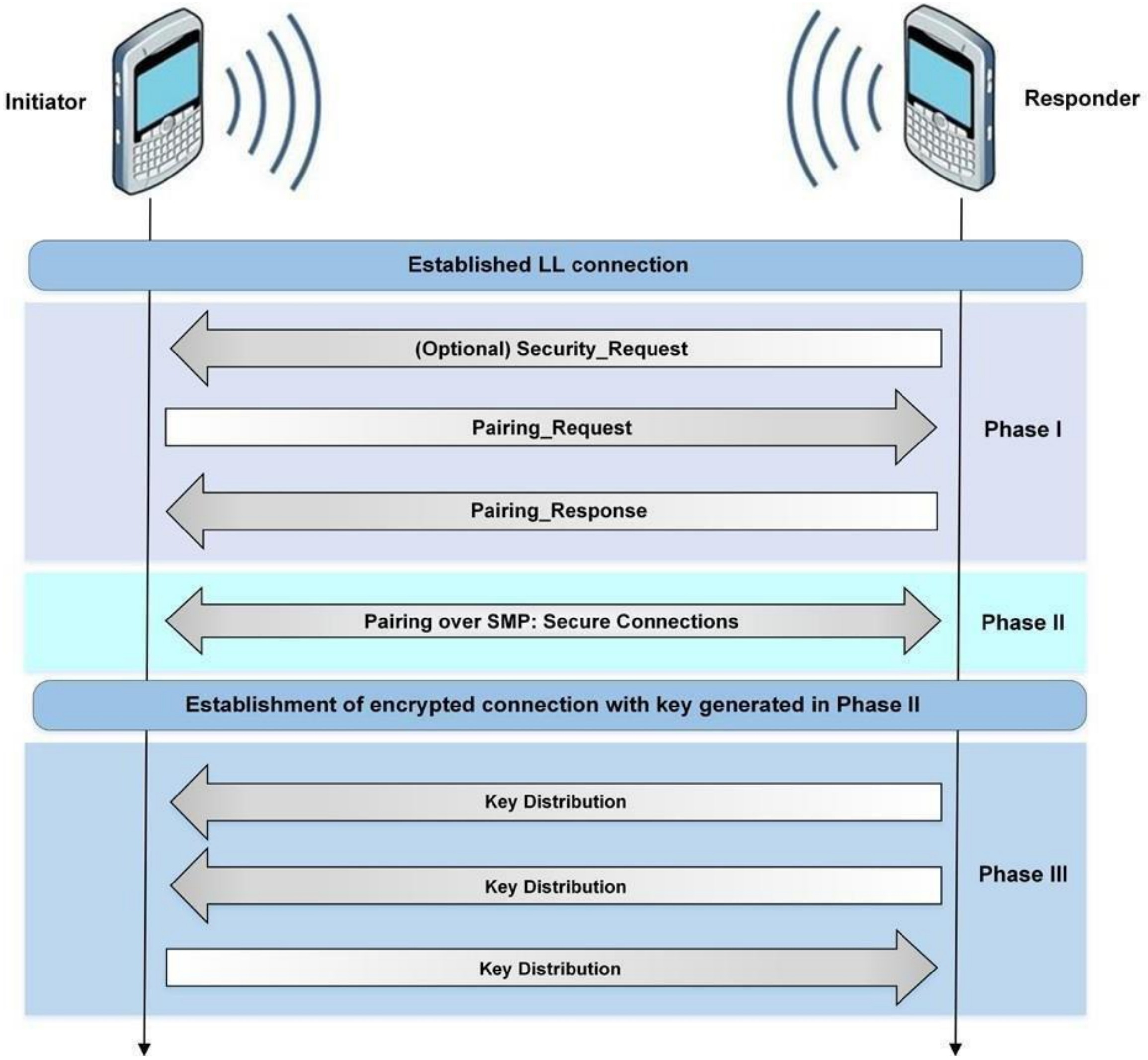

Initiator
Responder
Established LL connection
(Optional) Security_Request
Pairing_Request
Pairing_Response
Phase I
Pairing over SMP: Secure Connections
Phase II
Establishment of encrypted connection with key generated in Phase II
Key Distribution
Key Distribution
Key Distribution
Phase III

Figure 4.5: BLE Secure Connection Pairing [31]

There are four association models of pairing that both legacy pairing and secure connection use. The four models are numeric comparison, passkey entry, just works, and out-of-band (OOB) [31]. Each model is dependent upon the input/output (I/O) capabilities of the BLE device.

Numeric comparison works with secure connection pairing when both BLE devices have a display screen with a form of input (e.g., keyboard) [31]. A 6-digit number is displayed on each screen and the user must enter a “yes” response if the numbers match, if the user enters “no” then the pairing fails [31]. Passkey entry works when one BLE device has a display but no input capability, and the other has input capability but no display [31]. The BLE device with the display shows a 6-digit number that is used to enter in the BLE device with input capability [31]. Just works was designed when one BLE device does not have a display and input capability. Thus, the connection is accepted without confirming the value on both devices [31]. This makes the just works model susceptible to MITM attacks since the devices are paired insecurely.

Out of band pairing is for BLE devices that pair through another wireless protocol other than Bluetooth. The most common example of OOB pairing is near field communication (NFC), where two BLE devices discover and exchange cryptographic information from being in extremely close physical proximity to one another [31]. The user must then approve the connection before pairing. The security level of OOB is dependent on the developer of the OOB device, so MITM protection can be implemented [31]. A common example of NFC is current debit/credit card technology where all that is required for a transaction is a tap of the card onto a card reader. This capability is applicable to BLE for the pairing and key exchange process.

While BLE has some built in security to reduce MITM attacks and eavesdropping, there are still vulnerabilities and threats to be aware of. The just works model of pairing is highly insecure as it does not provide MITM protection, generating an unauthenticated key link [31]. It is also important to ensure that the BLE devices use the same mode and level of security. Security mode

4 devices can use lower security modes if the other BLE device does not support security mode 4. Lowering security modes poses risks as security mode 1 does not use any authentication or encryption methods, leaving the device completely vulnerable to attackers.

Bluetooth uses challenge-response authentication. Each BLE device takes the role of claimant or verifier; the claimant being the device proving its identity and the verifier confirming it by verifying the secret Bluetooth link key [31]. Imagine that to get into a secure building, you (the claimant) must know the secret password to verify that you are authorized to gain access. The guard at the door (the verifier) must verify that you are allowed access. If you say the correct secret password, you are allowed entry, and if you get it wrong you are denied. Bluetooth challenge-response authentication in principle works similarly, although much more complex in practice.

One issue with the challenge-response authentication process is that the challenge requests are unlimited, which could potentially compromise the secret link key. A malicious attacker could attempt to send multiple challenge requests repeatedly and potentially gather information about the secret link key [31]. Link keys also need to be stored properly. Link keys can be read or altered by an attacker if there are not sufficient access control mechanisms [31].

Another Bluetooth vulnerability is the lack of user authentication. While the devices authenticate, there is no method within Bluetooth to ensure the correct user is the one pairing the devices. There is also no end-to-end security innate to Bluetooth. Only the links are individually authenticated andencrypted, and data is decrypted at the link layer before being sent up the layers

[31]. End-to-end security methods to protect the data at every step must be employed by additional securitycontrols on top of the Bluetooth protocol stack [31].

While Bluetooth is susceptible to general attacks like MITM, eavesdropping, denial of service (DoS), etc., it also faces threats specific to Bluetooth. Bluesnarfing exploits firmware in older Bluetooth devices that forces a connection [31]. The attacker can access all the information stored on the victim device and can even route information to the malicious device [31].

Bluejacking is an attack that repeatedly sends messages or data to a device, usually a smart phone. The messages themselves are not harmful, but bluejacking can still cause the device to appear as it is malfunctioning. Bluejacking is akin to spam and phishing emails.

Bluebugging is an attack that is similar to bluesnarfing, it exploits firmware in older devices and can “bug” the device, allowing the attacker to listen to transmissions and manipulate the device [31]. BLE legacy pairing is also threatened by eavesdropping. An attacker can listen to the device pairing and can determine the secret key given enough time [31]. This vulnerability allows the attacker to impersonate a trusted device to the victim device. These vulnerabilities are not exhaustive but are relatively common and easy to exploit by threats.

To mitigate Bluetooth threats and vulnerabilities, there are certain measures an organization should consider before employing Bluetooth. Understanding the architecture and process of Bluetooth is necessary to implement security measures. Bluetooth devices should also be changed from their default settings to comply with the security policies [31]. Bluetooth devices should also remain at the lowest required power level and range to reduce the risk of detection by an attacker [31]. The just works model of pairing should be avoided since it does not use encryption or authentication to prevent MITM attacks. The devices without I/O capability should not be used if there are other available devices that can use OOB, numeric comparison, or passkey pairing models [31].

Bluetooth devices by default should remain undiscoverable until pairing to prevent discovery by an attacker. Pairing should also be performed as little as possible and only when necessary. Link encryption should always be active, and encryption should occur at every point of data communication [31]. Encryption keys should also use the maximum length possible to protect from brute force attacks, i.e., the longer the key size the more difficult it is to decipher [31].

As briefly mentioned earlier, BLE does not include end-to-end authentication and encryption, so ensuring there is a method for application layer security is necessary for sensitive data. Frequently patching devices is also crucial to ensure the device is up to date. Bluetooth should also make use of multi-factor authentication and strong password requirements. Overall, BLE is an efficient and decently secure standard for IoT, but it is not the only one. IoT devices can also communicate through cellular networks, particularly long-term evolution (LTE).

4.4 LTE Technology and Security

Many IoT devices, such as the two medical devices examined later in this paper, have wireless cellular capability. Cellular networks are wireless networks that provide coverage for an area using cellular sites made up of radio equipment [32]. A cellular site can be owned by a telecommunications company, and internet service provider (ISP) or a government entity. The owners of a cellular site are known as Mobile Network Operators (MNOs) [32]. The MNOs distribute the radio equipment for cellular sites and connect them to a core network the MNO operates [32].

LTE allows mobile devices to utilize IP networks for transmission. LTE provides mobility, meaning that IP connectivity is maintained when moving from tower to tower [32]. LTE is useful for IoT devices because it offers a mobile method of communication without requiring a connection to WiFi or a wired network. The architecture of LTE includes the User Equipment (UE), the Evolved Universal Terrestrial Radio Access Network (E-UTRAN), the Evolved Packet Core (EPC, also called the core network), and the IP network. Figure 4.6 illustrates the basic architecture of LTE.

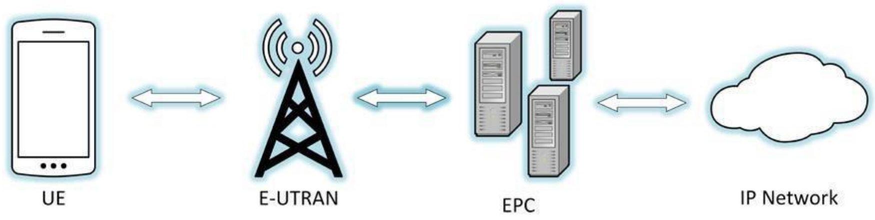


Figure 4.6: The Architecture of LTE [32]

Mobile devices like smart phones and tablets in LTE networks are referred to as user equipment. They are the predominant end points in LTE networks [32]. UE consists of the OS and a hardware chip called the Universal Integrated Circuit Card (UICC) that is responsible for accessing the cellular network [32]. The UICC runs a Java application called the Universal Subscriber Identity Module (USIM) that connects with the cellular radio and IP network [32]. To identify a mobile device as a subscriber to the cellular network, LTE uses two methods: the International Mobile Equipment Identifier (IMEI) and the International Mobile Subscriber Identity (IMSI). The IMEI is essentially a serial number for the mobile device and the IMSI is a unique number assigned to the device's UICC. The LTE network verifies the mobile device and determines which services to provide through these methods.

The E-UTRAN is a mesh network of cell towers, known as base stations [32]. The E-UTRAN is responsible for receiving radio signals from UE and translating them into IP packets to send to the core network [32]. Base stations are enabled to hand off communication to one another based on the UE location. This mobility provides seamless and uninterrupted connectivity. The EPC is responsible for the routing and computing capability of LTE [32]. The connection between the radio network and the EPC is called the backhaul [32]. There are many technical components to the EPC that are beyond the scope of this paper. It is important to know that LTE has specific protocols that operate on either the user plane or the control plane: "The user plane is the logical plane responsible for carrying user data being sent over the network (e.g., voice communication, SMS, application traffic) while the control plane is responsible for carrying all of the signaling communication needed for the UE to be connected" [32].

For LTE security, the UICC plays a major role. One of the functions of the UICC is to store cryptographic keys and other credentials [32]. The UICC is provided with a long-term key shared between the UICC and the MNO [32]. The long-term key is used to create other keys in the cryptographic process [32]. LTE uses a variety of encryption methods, including AES-128 and AES-256. To authenticate a UICC on the LTE network, the Authentication and Key Agreement (AKA) protocol is used [32]. The AKA protocol verifies the long-term key shared between the UICC and the MNO, providing authentication for the UICC on the LTE network [32]. It is worthy to note that the UICC can be removed from the device, so the AKA cannot authenticate the user or the device itself.

There are many threats and vulnerabilities in LTE networking due to the complex nature of communication. The communication between the UE and base station is through radio frequency over the air (also called the Uu interface), which is not always private [32]. The user plane packets traveling through radio frequency do not have integrity protection [32]. Thus, the Uu interface is vulnerable to eavesdropping. It is also an optional configuration for the packets in both the user plane and control plane to provide confidentiality protection in the Uu interface, this is for the operator of the LTE network to determine [32].

The IP communications from the base station to the core network can be intercepted if there are no security measures. The use of security measures like IPsec between the base station and the core network provides authentication, confidentiality, and integrity protection for IP packets [32].

IPsec is a security mechanism for IP networking that provides an encrypted connection through the Authentication Header protocol (AH) and Encapsulating Security Payload (ESP) [33]. The authentication header protocol ensures the data is from its original source by using data integrity checks [33]. The encapsulating security protocol encrypts the packet by using the Internet Key Exchange protocol to determine how to protect the information being exchanged [33]. The IKE sets the security associations, the parameters, and agreements on which algorithms, protocols, and keys are used [33].

The UE themselves are susceptible to malware attacks. Malware can infect the OS of mobile device and cause a loss of service [32]. Malware can also cause UE to be a part of a botnet attack, forcing the UE to continually send requests over radio frequency to the E-UTRAN [32]. To reduce malware attacks, patching is important. Patching provides up-to-date protection of the UE. Rogue base stations are also a threat to LTE security. A rogue base station is one that is not owned or operated by an MNO [33]. The rogue base station can cause the UE to communicate with it and force it to use a weaker cellular communication (e.g., 2G) [32]. Figure 4.7 illustrates a downgrade attack.

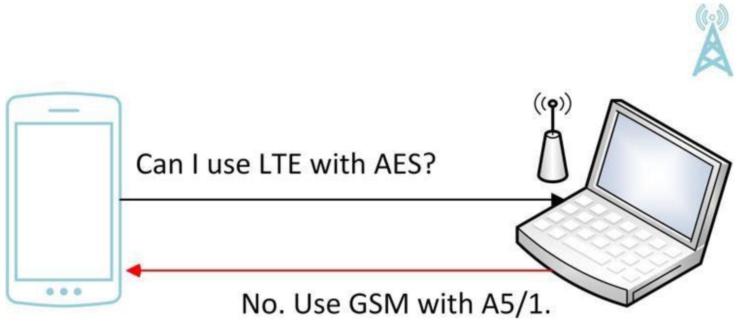


Figure 4.7: Rogue Base Station Downgrade Attack [32]

There are several mitigation techniques that can be used to secure LTE. Cryptographic protection can be enabled by the operator to prevent Uu interface eavesdropping [32]. Using IPsec for core network and base station communication provides confidentiality, integrity, and authentication [32]. Providing physical security of the UE and the core network infrastructure is important to protect equipment. Patching the UE provides up-to-date protection to mitigate malware attacks.

The UICC can be protected by giving the UICC a PIN that only the user knows, this ensures that the user is authenticated with the device [32]. There are also methods to detect rogue base stations, such as providing a list of trusted base stations and allowing the user to determine if they wish to connect [32].

LTE security is a complex issue that requires knowledge of IP networking and security because of the integration with cellular communication. There are many points of access in LTE, from the UE to the E-UTRAN to the core network. A communication chain is only as strong as its weakest link, so protecting each point requires thorough consideration and knowledge. LTE security is necessary, especially for sensitive information, such as ePHI.

Chapter 5. Privacy and Security Concerns of IoT in Healthcare

This chapter explores the privacy and security concerns of ePHI in IoT. The collection of personal information in IoT requires adequate protection. There are regulations in healthcare that must be followed, such as HIPAA. The Health Information Technology for Economic and Clinical Health Act (HITECH Act) is a part of HIPAA that is necessary to understand as a part of healthcare information technology. The risk of compromising ePHI is high. Violations of these regulations can result in a range of punishments from fines to loss of licenses. It is in the best interest of the healthcare organization to ensure there is adequate security protecting ePHI.

5.1 Overview of HIPAA Rules and ePHI

HIPAA is a federal law created in 1996 to provide a set of standards for protecting sensitive patient information [34]. The goal of HIPAA is to prevent unwanted disclosure of protected health information (PHI) of patients [34]. PHI consists of medical records and information that can identify an individual (age, sex, height, weight, birth date, etc.). HIPAA protects patients by enforcing regulations on covered entities. Covered entities are healthcare providers, healthcare plan providers (i.e., entities that pay the cost of medical care), healthcare clearinghouses, and any business associate (other persons or organizations that uses PHI to provide a service) [34]. The privacy rule of HIPAA seeks to provide adequate protection of patient information while enabling covered entities to transmit and access necessary patient information [34]. Striking a balance between privacy and efficiency is a goal of the privacy rule of HIPAA.

The HIPAA security rule is similar to the privacy rule, but it protects all PHI collected, maintained, and transmitted in an electronic format (ePHI) [34]. Thus, the security rule does not apply to any written or spoken PHI. The security rule addresses the administrative, physical, and technical safeguards used to secure ePHI [35]. The confidentiality, integrity, and availability of ePHI is necessary to maintain to remain compliant with HIPAA rules.

Administrative safeguards are policies and procedures of a covered entity that address the actions taken to protect ePHI [35]. For example, staff training and education is an administrative safeguard. Physical safeguards are the measures to protect the physical equipment from unauthorized access [35]. An example of a physical safeguard is securing the computer systems through an electronic badge reader to verify credentials. Technical safeguards are the most complex and difficult to implement [35]. Technical safeguards encompass the technology and practices used to secure ePHI. An example of a technical safeguard is using Virtual Private Network (VPN) to securely transmit ePHI over an otherwise insecure network.

To maintain compliance with the HIPAA security rule, covered entities are also required to conduct a risk assessment [35]. A risk assessment is used to evaluate the threat landscape of an organization and implement security measures to mitigate risk. Each covered entity is different and has its own set of policies, procedures, and infrastructure. HIPAA is not concerned with how compliance is maintained, just that it needs to be, and it needs to be documented [35].

5.2 The HITECH ACT

The HITECH Act was signed into law in 2009 as an additional act under HIPAA. The HITECH Act was created to replace paper record with electronic health records (EHRs) [36]. Paper records were largely inefficient and cumbersome when the technology for EHR was available, albeit expensive. To assist with the adoption of EHRs, covered entities were given financial incentives to transition to EHRs [36]. In addition to providing incentives, it also provided stricter guidelines for HIPAA rules, ensuring that patients were notified of a violation and provided harsher penalties for violations [36].

The financial incentives coupled with increased penalties strongly encouraged covered entities to adopt EHRs. The civil penalties for a violation before the HITECH Act was a $100 fine per violation up to a maximum of $25,000 [36]. The penalty system was revised with the HITECH Act, creating tiers of penalties based on severity. The penalties are split into four tiers, tier 1 being the least egregious and tier 4 being the most. Tier 1 violations are those where a covered entity is unaware of a HIPAA violation and would not have reasonably known [36]. Tier 4 violations are those where there is willful neglect of HIPAA rules and no corrective action to rectify it within 30 days [36]. The maximum fine for a HIPAA violation was increased to $1.5 million [36]. Table 5.1 below illustrates the HIPAA violation tier system adjusted for inflation.

Table 5.1: HIPAA Violation Tier System [35]

Culpability	**Minimum Fine/Violation**	**Maximum Fine/Violation**	**Annual Penalty Cap**
Tier 1: **No Knowledge**	$120	$60,226	$1,806,757
Tier 2: **Reasonable Cause**	$1,250	$60,226	$1,806,757
Tier 3: **Willful Neglect-Corrected**	$12,045	$60,226	$1,806,757
Tier 4: **Willful Neglect–Not Corrected**	$60,226	$1,806,757	$1,806,757

One of the major benefits of the HITECH Act was enforcing HIPAA rules on business associates and crimping the loophole of plausible deniability [36]. Previously, covered entities could claim that they were unaware that the business associate was not HIPAA compliant, avoiding the sanction [36]. The HITECH Act curbed this by including the business associate as a covered entity and enforcing HIPAA rules. Additionally, The HITECH Act made it mandatory for covered entities to send a notification to those who had their information breached, known as the Breach Notification Rule [36].

To improve transparency, the Office of Civil Rights (OCR) created a list of covered entities who had violated HIPAA rules and display it on their website [36]. The HITECH Act also increased patient rights by allowing patients to access their EHRs and request copies [36]. The HITECH Act is important for IoMT because it laid the groundwork for it to evolve. Since the Act caused the transition of covered entities from paper records to EHRs, healthcare IT and technological developments boomed. The HITECH Act also directly relates to IoMT because IoMT collects, transmits, and stores ePHI. Thus, every covered entity that uses information relating to IoMT must remain HIPAA compliant. With the transition, it was necessary for covered entities to improve their security measures to protect ePHI.

5.3 The Risk of Compromising ePHI

As with any information technology system, there will be a risk that data is breached or compromised. In the healthcare setting, the risk is severe due to the sensitive, personal, and financial information of people. According to NIST, risk is defined as: “a measure of the extent to which an entity is threatened by potential circumstance or event and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” [37]. Risk weighs the likelihood of an attack as well as the loss that would occur if an attack occurred. There may be a high likelihood of an attack occurring, but if it does not result in loss then the risk may be classified as low. It is important to understand that risk varies for every organization. A threat for one entity may not be a threat for another.

The compromise of ePHI can be a disastrous situation for covered entities because of HIPAA rules and potential sanctions that follow if there was a violation. Not only are there sanctions, but there is a loss of reputation and trust with the people they service. Indeed, when conducting a risk assessment, it is important to consider the impact a risk would have on community perception and trust. HIPAA sanctions result in civil penalties and can also lead to criminal penalties. If a healthcare professional knowingly uses patient data in a manner outside of HIPAA guidelines, they are potentially susceptible to criminal penalties [38]. Examples of criminal HIPAA violations are stealing patient data for profit and disclosing PHI with malicious intent.

Table 5.2: HIPAA Criminal Penalty Tiers

Tier 1	No knowledge of violation	Up to 1 year in jail
Tier 2	Obtaining PHI under false pretenses	Up to 5 years in jail
Tier 3	Obtaining PHI for personal gain or with malicious intent	Up to 10 years in jail

Some of the most common HIPAA violations are snooping on ePHI/PHI, failure to conduct risk assessment/management, denying patients' access to records, lack of ePHI controls (authorization), failure to encrypt or otherwise protect ePHI, wrongful disclosure of PHI, and improper disposal of PHI [38]. It is common that a covered entity that lacks a risk assessment and risk management process and is subjected to sanctions and must take corrective action. At the individual level, snooping and wrongful disclosure occur frequently [38]. HIPAA rules do not require encryption to be used for ePHI but covered entities must have an equally sufficient method for protection [38]. For IoMT, having sufficient ePHI controls and encryption are the most important. With the many points of transmission and routes ePHI can take in IoMT, it is imperative that covered entities have measures in place to protect ePHI in IoMT.

A case in 2020 shows the importance of safety measures. An ambulance company lost an unencrypted laptop containing ePHI of over 500 patients [39]. In the ensuing investigation, it was found that the ambulance company were in violation of multiple HIPAA rules. [The ambulance company] "had not conducted a comprehensive, organization-wide risk analysis (45

C.F.R. § 164.308(a)(1)(ii)(A)), had not implemented a security awareness training program for its employees (45 C.F.R. § 164.308(a)(5)), and had failed to implement HIPAA Security Rule policies and procedures (45 C.F.R. § 164.316)" [39]. The OCR aided the company, but despite the help it was found that the ambulance company had not taken meaningful action to correct the problem resulting in a fine of $65,000 [39]. In addition, the ambulance company was placed under HIPAA scrutiny for two years to ensure they maintained compliance [39].

There are many points of attack in a healthcare setting that make it difficult to protect. From phishing and social engineering that obtain user credentials for unauthorized access, to ransomware that holds information hostage until a dollar amount is paid, there are many threats to assess in the healthcare setting. With IoMT becoming ubiquitous, this risk is amplified. Not only is the healthcare organization concerned with their information systems, but in the case of remote patient monitoring, now the patients themselves must be aware of potential cyber threats.

Chapter 6. Implementation of IoMT on Real Devices

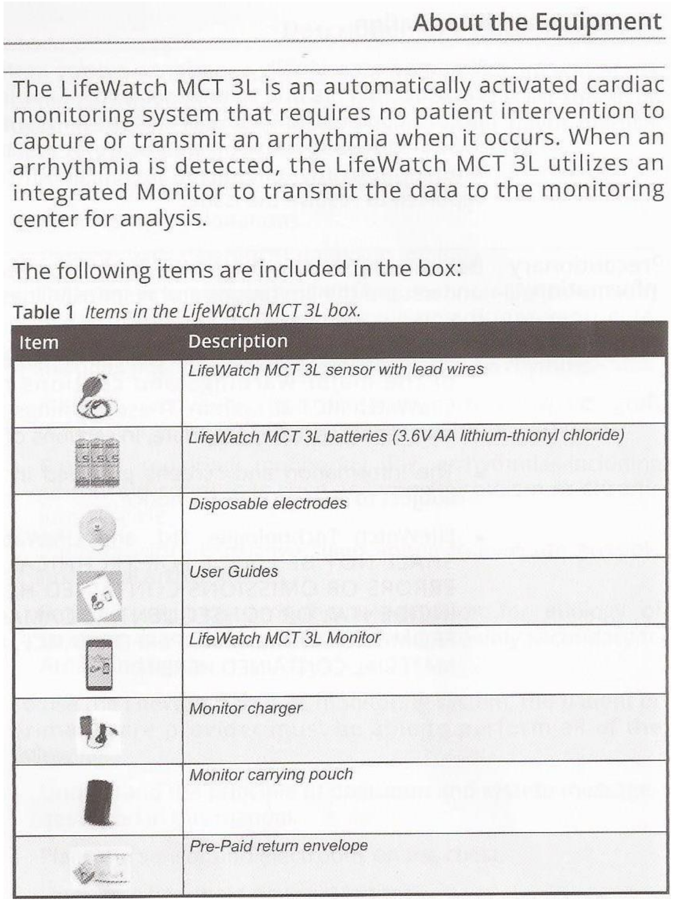
This chapter is the examination of two implementations of IoMT. First, I will describe how the IoMT implementations work and then present my answers to the research questions. The LifeWatch Mobile Cardiac Telemetry 3 Lead (MCT3L) device, and the remote patient monitoring system from Vivify Health are the two IoMT applications I selected as research subjects for this thesis.

6.1 Research Questions on IoMT Implementation

1. What communication protocol does the IoT device use (Bluetooth, WiFi, Cellular, etc.)? If they use Bluetooth, which version?
2. What data protocol does the IoT device use (CoAP, MQTT, AMQP, etc.)?
3. What encryption methods do they use for data-at-rest and data-in-transit, if any?
4. Is biometric data stored locally on the IoT device? If so, is it encrypted?
5. What security measures does the IoT device manufacturer/provider implement (e.g., multi-factor authentication, use of secure cloud, etc.)?
6. What are the current security controls used to protect these IoT devices?
7. What does the IoMT architecture look like?
8. What are some of the risks if the device is compromised?
9. Are there any security flaws in protecting these IoT devices?
10. To improve the security of these IoT devices, what are some suggestions to protect these IoT devices?

6.2 LifeWatch Mobile Cardiac Telemetry 3 Lead (MCT3L)

The MCT3L device is a device for continuous ECG monitoring and arrythmia detection [40]. This device is issued to patients with symptoms of cardiac arrythmia for remote monitoring [40]. The device monitors patient ECG and automatically detects cardiac arrythmia based on an algorithm, which alerts the patient and records the data [40]. Arrythmia events can also be recorded manually by the patient and transmits the ECG data to a monitoring center [40]. The monitoring center then presents the data to the healthcare provider [40]. The following figure from the Patient User Guide illustrates and describes the equipment.



About the Equipment

The LifeWatch MCT 3L is an automatically activated cardiac monitoring system that requires no patient intervention to capture or transmit an arrhythmia when it occurs. When an arrhythmia is detected, the LifeWatch MCT 3L utilizes an integrated Monitor to transmit the data to the monitoring center for analysis.

The following items are included in the box:

Table 1 *Items in the LifeWatch MCT 3L box.*

Item	Description
	LifeWatch MCT 3L sensor with lead wires
	LifeWatch MCT 3L batteries (3.6V AA lithium-thionyl chloride)
	Disposable electrodes
	User Guides
	LifeWatch MCT 3L Monitor
	Monitor charger
	Monitor carrying pouch
	Pre-Paid return envelope

Figure 6.1: LifeWatch MCT3L Equipment [40]

The monitor, which is a handheld device, received the ECG data from the sensor via Bluetooth [40]. The monitor can also store up to 30 days of data [40]. The monitor runs on a proprietary application that translates the ECG data and sends it over cellular networks to the monitoring center [40]. The sensor records and transmits ECG data to the monitor [40]. The sensor is battery powered (3.6V AA lithium-thionyl chloride) and uses four disposable electrodes that are placed on specific areas of the human body which connect to the sensor's lead wires [40]. The three figures below illustrate the MCT3L system. Figure 6.2 illustrates the sensor, wires, monitor, and electrodes. Figure 6.3 illustrates the electrode placement. Figure 6.4 illustrates the communication between the sensor and monitor.

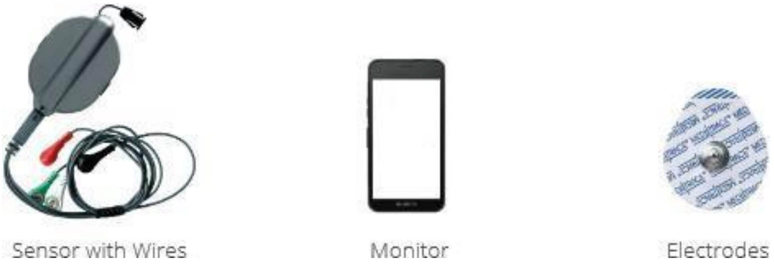
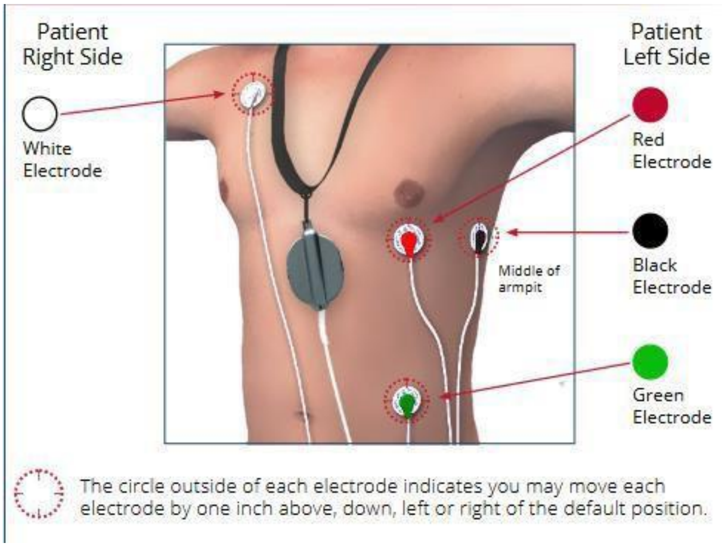


Figure 6.2: MCT3L Components [41]



The circle outside of each electrode indicates you may move each electrode by one inch above, down, left or right of the default position.

Figure 6.3: MCT3L Electrode Placement [41]

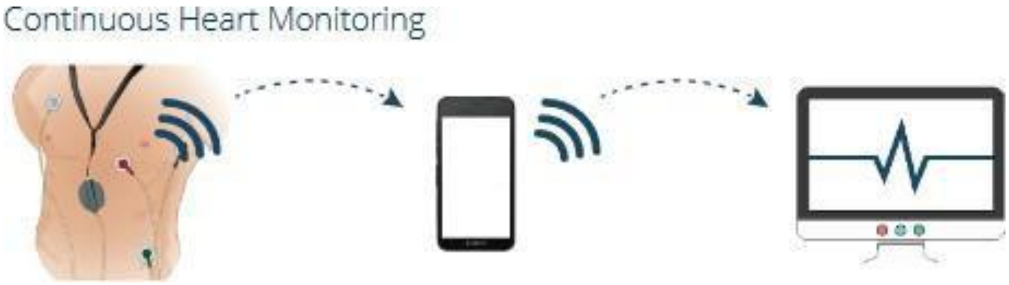


Figure 6.4: MCT3L Communication [41]

Since the sensor and monitor communicate via Bluetooth, they must be in a specific range of each other (30 feet) for data to be transmitted to the monitor. The sensor also has a flash buffer memory for storage, a specialized circuit for ECG signals, a Bluetooth transceiver, and a buzzer [40]. The sensor can loop up to 6 hours of ECG recordings in the flash memory to preserve the data when the Bluetooth link to the monitor is down (e.g., out of range) [40].

The MCTL3 uses the Bluetooth serial port profile (SPP), which emulates a serial cable connection between two devices. I was unable to determine which exact version of Bluetooth the devices use. However, SPP is based off the RFCOMM protocol, which is a simple transport protocol that is unsupported by BLE, thus the devices use Bluetooth classic.

6.3 Answering Research Questions for the LifeWatch MCT3L Device

As mentioned earlier, the MCT3L uses the SPP of Bluetooth classic to communicate between the monitor and the sensor. The monitor sends the ECG data over cellular networks (LTE) to transmit the data in the form of IP packets to the monitoring center. There is no information in the user guide about a data protocol but based on the information given, it does not use a data protocol. The entire system of the MCT3L is a WBAN that transmits ECG data from the monitor solely through cellular networks, where Bluetooth collects information from the sensor and LTE does the legwork for communication to the monitoring center.

The Patient User Guide does not discuss encryption methods, but it is safe to determine that data stored on the sensor until a Bluetooth link with the monitor is established is not encrypted. The reason being that the sensor is a low-power device that uses flash memory to store the ECG data. The sensor likely does not have the computational power required to perform encryption.

For data-in-transit, the data is encrypted using the LTE standards. It is worth noting that it is unknown if the data is encrypted while being transmitted to the base station; the data may only be encrypted from base station onward to the core network by the default LTE standard.

The first-time set up for the MCT3L requires the patient to call a LifeWatch technician for set up. Based on this information, it is safe to assume that the technician must approve the user and activate the device. Once the device is activated, however, there is no password protection to access the monitor. This is because the monitor and sensor are on 24/7 for the entire time the devices are being used (30 days).

This device and user are approved by the LifeWatch technician for set-up, but there are no following security controls to authorize the user. There is nothing to ensure that the intended patient is the one using the device. Hypothetically, a curious relative of the patient could equip the electrodes and sensor, providing inaccurate ECG data of the intended patient. There is no encryption at rest due to the continuous monitoring and communication between the monitor and sensor.

The MCT3L devices send data over cellular networks, where LifeWatch collects the data and presents it to the healthcare providers, where they have a portal to access. The healthcare network authorizes the communication between itself and the telehealth provider. The firewall must be configured to allow traffic from the telehealth provider into the private hospital network.

The risk if the device is compromised is high. The device being compromised can result in the violation of confidentiality, integrity, and availability, resulting in loss of trust from the patient and other potential penalties. MITM attacks, eavesdropping, ransomware, and phishing are all threats that could exploit a vulnerability in the device or user, leading to severe negative outcomes such as loss of trust and financial loss.

Because the device uses Bluetooth classic instead of BLE, it lacks some of the key security features that BLE inherently provides. The device likely pairs with the just works association model because of the lack of I/O capability in the sensor. If this is the case, it does not provide any MITM protection. It is also susceptible to botnet and DoS attacks because of the simple Bluetooth communication. A DoS attack would greatly impact the service of the device. Other major flaws include a lack of encryption for data stored in the sensor. This data could potentially be seen or stolen by an attacker if they can force the sensor to pair with the attacker (bluensarfing/bluejacking). It is unknown what security parameters are initiated upon set-up with the technician. It is possible the sensor is programmed to only trust the monitor in the initial pairing, but a competent attacker could still forcibly pair with the sensor.

This device is outdated and thus highly susceptible to common Bluetooth attacks. The organization should use a modern Bluetooth device that is BLE capable. BLE provides more inherent protection and additional security measures can be added on top of BLE. While BLE is still vulnerable, it is considerably more secure than Bluetooth classic. If not BLE, at the very least increase the security level/mode and use a different pairing scheme other than just works.

It is suggested to use a different sensor that has the computing power to encrypt the ECG data-at-rest and allow for additional encryption for data-in-transit and allow for a different pairing scheme. Lightweight encryption methods exist, such as the Lightweight Encryption Algorithm (LEA) for WBANs [42]. It is also suggested to include password protection, ideally multi-factor authentication (MFA) for the monitor. Password protection with MFA reduces the likelihood that someone other than the intended patient is using the device.

6.4 Vivify Health Remote Patient Monitoring System

The Vivify Health RPM system includes a Samsung Galaxy Tab E 32GB tablet, and three BLE capable sensing devices: a sphygmomanometer, a pulse oximeter, and a weight scale. The sphygmomanometer is used to detect blood pressure, the pulse oximeter measures the amount of oxygen in the blood, and the weight scale detects weight by standing on it. The sphygmomanometer provides the patient with a blood pressure cuff and collects the reading. The pulse oximeter is a Bluetooth device that the patient places on their finger. Light beams from the pulse oximeter read the oxygen levels without having to draw blood. The weight scale records the weight after use. Figure 6.5 below illustrates the RPM kit.

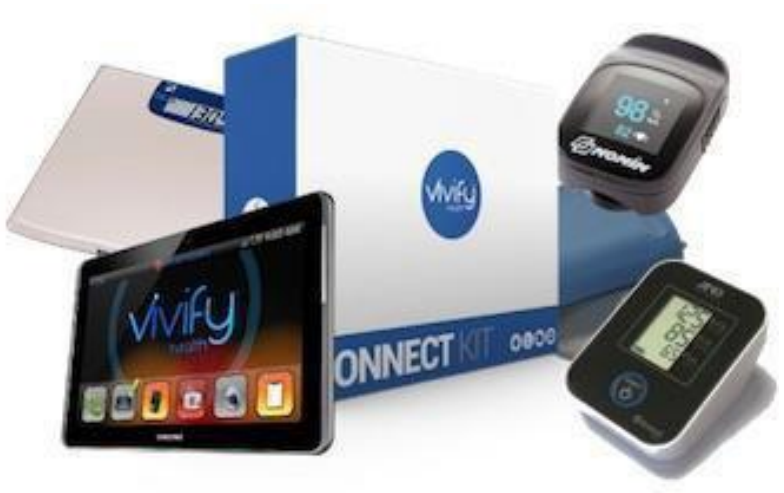


Figure 6.5: Vivify Health Remote Patient Monitoring Kit [43]

The sensing devices collect biometric data and send it via cellular network or WiFi to the telehealth provider, Vivify Health, who presents the data to the healthcare organization. The Samsung tablet houses the applications for the devices and acts as the gateway for communication. Specifically, the Samsung tablet receives biometric readings from the medical devices using Bluetooth 4.0. Then, the biometric data is sent to the servers using RESTful API services. The data is encrypted at rest using AES-256 and protected using TLS while in transit. TLS is the security protocol used in HTTPS to ensure internet communication is encrypted. The data is stored and encrypted on the device until confirmed it has been received by the server.

Bluetooth connectivity is password protected and OAuth 2.0 Token authentication is used to secure the servers. OAuth 2.0 is a protocol that allows a user to permit a third-party access to protected resources.

There are four roles in the OAuth 2.0 process. The resource owner is the owner of the protected resource (in this case Vivify Health) who authorizes an application to access the account [44]. The client is the one making access requests to access the protected resources [44]. The authorization server issues the access tokens after authenticating the resource owner and grants authorization to the client [44]. The resource server is the server housing the protected resources [44]. The resource server responds to requests using access tokens [44]. In this case, Vivify Health is the resource owner and the client requesting access is the healthcare organization. The OAuth 2.0 token process provides secure access by authenticating Vivify Health as the resource owner and authorizing the healthcare organization. Figure 6.6 illustrates the OAuth2.0 protocol.

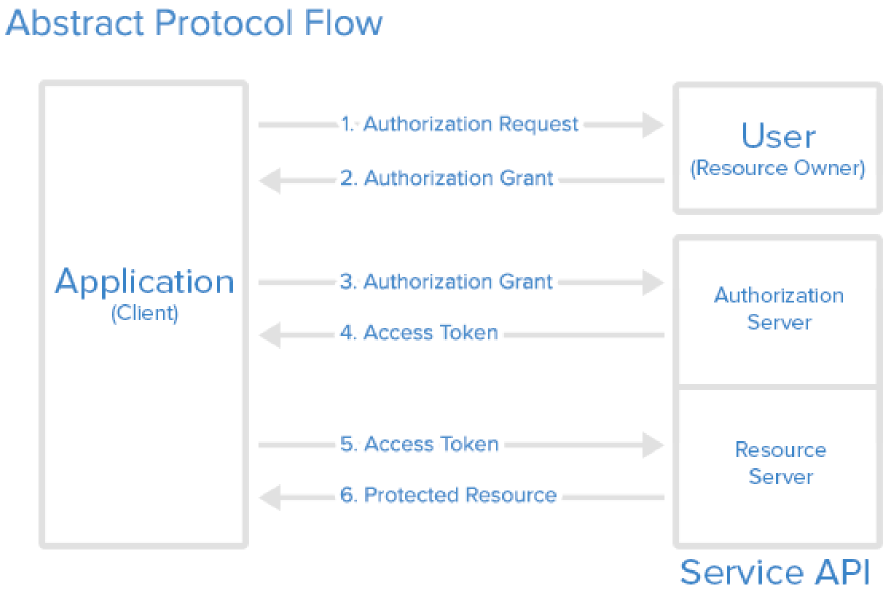


Figure 6.6: The OAuth 2.0 Protocol [45]

In addition to the OAuth 2.0 protocol, a 4-digit PIN code is required to login to the device and all devices are locked down using Mobile Management Software. The risk of the RPM system being compromised is moderate. There are security measures in place like encrypting data-at-rest and in-transit that reduce the likelihood of a breach. The devices all use a modern version of Bluetooth (BLE) which bolsters the security compared to Bluetooth classic. BLE ensures there is MITM protection, and the devices securely authenticate one another. However, if the RPM system is compromised through phishing, ransomware, or other common methods, it could result in a loss of confidentiality, integrity, and availability. There is a plethora of sensitive information that could result in loss of patient trust.

While the devices communicate vie BLE, the Samsung tablet is WiFi capable, meaning that the information is being sent from the patients' home network or other insecure networks depending on the patient's location. A home network may not be configured to provide the best possible security, so to solve this problem it is possible to segment the patient home network from the RPM devices. End-to-end protection is vital for an RPM system to ensure utmost security of sensitive data.

Separating other devices in a home network from RPM devices can be accomplished with using a layer 2 over 3 solution, this secure separation is called an enclave [46]. Layer 2 refers to the data link layer (e.g., ethernet) in the OSI model and layer 3 is the networking layer (e.g., router). Cawthra, et al. [46], have emulated this by creating a lab that segmented patient home networks. Threats to home networks can be mitigated, preventing unauthorized remote access to RPM devices. The layer 2 over 3 solution would be provided by the telehealth provider (i.e., Vivify

Health). The provided solution could be a secure gateway that provides layer 2 over layer 3 security. The enclave solution ensures the RPM devices in the patient home network remains separated and inaccessible from the rest of the patient home network.

The Samsung tablet also uses weak password protection. The tablet should use a PIN longer than 4 digits and include MFA. This would ensure that the tablet itself is more secure from physical tampering, in the case it is lost or stolen. While data-at-rest is encrypted, it is still undesirable for the tablet to be accessible to someone other than the intended patient. No data is stored on the sensing devices. All biometric data is communicated via BLE to the Samsung tablet. The tablet has plenty of storage space for data and computing power to perform encryption.

Chapter 7. Solutions and Countermeasures for IoT Security Issues

This chapter explores some additional security countermeasures that are useful for IoT. Understanding the device manufacturer’s role in security, establishing security policies and procedures, and providing education and awareness of all users are all countermeasures that can make IoT a secure environment. Lightweight encryption methods are being developed to help ease the burden of computational power, and with the advent of blockchain technology, IoT data can be secured with it. The cloud is also a useful tool for IoT security. Using a private cloud to house the enormous amount of IoT data provides convenience for authorized parties.

7.1 General Security Countermeasures

7.1.1 Manufacturer’s Responsibility

Currently, there is a huge gap in security in the development of IoMT devices. According to a survey by the HIPAA Journal [47], approximately half of the device manufacturers stated that security is considered as a factor during the design process. The majority (82%) of the manufacturers stated that they have major security concerns and felt that safeguards were lacking to protect from an attack [47]. Every IoMT device on the market must meet certain criteria by the FDA to be approved and deployed. It is the manufacturer’s responsibility to provide certain security countermeasures innately to ensure compliance. The manufacturer must understand the purpose of the IoMT device, the type of information it will collect, and the environment it will be operating in. It is the manufacturer’s responsibility to adequately develop and prepare IoMT devices for deployment. Understanding the needs of the clients/customers is necessary.

Manufacturers must address risk and risk mitigation techniques such as asset management, access management, vulnerability management, data protection, and incident protection [48].

Asset management is maintaining an accurate record and inventory of all IoT devices throughout the deployment life cycle [48]. This is important to ensure accountability of IoT devices. Access management is preventing unauthorized access of the physical device. Restricting access to IoT interfaces and applications mitigates risk of compromise [48]. The manufacturer can implement access management by providing rules to access applications and include MFA to access the device.

Vulnerability management is the general upkeep of the device, such as patching that provides up-to-date security and fixes operational issues [48]. Data protection refers to methods to protect data-at-rest and data-in-transit (e.g., encryption) to prevent exposure of sensitive information (e.g., ePHI) [48]. Incident detection is the monitoring of IoT device activity to detect any security breaches or compromise of data [48]. These are mitigation areas that manufacturers must keep in mind while developing IoT devices, especially in the medical field where sensitive personal information is collected. A lack of security in IoMT can lead to severe penalties from HIPAA, as exemplified by the case described previously in section 5.3. In that case, the HIPAA penalty was severe, they were fined above the minimum fine for tier 4 violations and were placed under scrutiny of the OCR for two years. This penalty greatly impacted the company financially with the fine and operationally by requiring OCR oversight. This case shows why proper security measures are important to maintain HIPAA compliance.

7.1.2 Robust Security Policies and Procedures

Creating guidelines for IoT device and information use is necessary, especially in the medical field. Having rules in place that dictate who can access what and for what purpose prevents unauthorized access and reduces the likelihood of the IoT device or information being compromised. Each covered entity in the healthcare sector that interacts with IoMT devices or information must follow HIPAA rules. To reach and maintain compliance, policies and procedures are written to provide rules and guidelines. A hypothetical policy example follows; only certified and authorized physicians may access the EHR of patients that use RPM systems. The physician must swipe their badge and provide a password to enter the EHR. This policy states that a) only authorized physicians may access the EHR of RPM patients and b) they must provide multiple active credentials in the form of electronic badge and password. This example policy reduces the likelihood of unauthorized access by dictating who can access the EHR and how to access it.

Other policies and procedures may go more in depth into the technical details, such as encryption methods. It is worth noting that not only would the healthcare organization implement policies and procedures, but also the telehealth provider. All RPM information is first sent to the telehealth provider for processing and presentation before the healthcare provider can access it. Each covered entity must have a robust security policy that provides rules and guidelines for security countermeasures.

7.1.3 Network Segmentation/Hardening

As mentioned earlier, network segmentation is useful for separating the RPM environment from a home network. Network segmentation is a useful security measure for the telehealth provider and the healthcare provider as well. Segmenting the EHR from the rest of the network provides additional security so that the ePHI cannot be accessed from within the main hospital network. Network hardening refers to security countermeasures that bolster network security. Network hardening can mean that firewall rules are configured more strictly to prevent additional traffic. Closing certain ports and using demilitarized zones (DMZs) to protect the internal network provides additional security. DMZs are used to separate the internal network from the public internet by housing the external-facing servers between firewalls. Disabling unused network services, implementing intrusion detection and prevention systems are all countermeasures to harden a network.

For IoMT, the best security countermeasures possible should be implemented to reduce the risk that ePHI is intercepted, manipulated, or stolen. These methods are commonly recommended and provide robust network security. Hardening and segmenting networks reduces the risk of common attacks like DoS attacks. An intrusion prevention system and advanced firewalls can prevent DoS and botnet attacks from disrupting services. If an attack like DoS does occur, a hardened network would be able to respond faster tothese threats, reducing loss.

Network segmentation provides an additional layer of security around the network's perimeter. This is how businesses can provide guest WiFi services without risking the protected resources. Network segmentation can be accomplished by physically separating the network, or logically with virtual local area networks (VLANS) to automatically route traffic to the correct subnet. Network segmentation should be used in healthcare to include IoMT devices. This will provide a secure perimeter in the healthcare organization's network to protect the information collected and sent by IoMT devices. IoMT information should be considered as a protected resource since it is ePHI. As suggested in this work, the patient’s home network should be considered as a potential vulnerability. Providing a segmented network for the patient’s IoMT devices can ensure that ePHI is secure. This is accomplished through a physical appliance to segment the IoMT resources. For the MCT3L and the RPM kit, implementing network hardening techniques will better protect the ePHI when accessed by the telehealth provider and the healthcare organization. The goal of network hardening/segmentation is to reduce the attack surface, thus reducing risk.

7.1.4 IoMT Security Training and Education

An administrative measure for securing IoMT, and just as important as technical and physical security countermeasures, is creating some means of IoMT training and education for staff. Healthcare professionals must have awareness of the risks involved with IoMT and understand that ePHI is necessary to protect. A covered entity should have training and awareness for its employees to always keep security in the forefront. For example, simulating phishing by sending emails organization wide can keep staff alert. Educating staff on what phishing looks like and how to report it can mean the difference between a hefty HIPAA fine and successfully protecting ePHI.

Education and training go hand in hand with security policies and procedures. There must be policies for keeping staff up to date on security awareness and training. New threats and vulnerabilities arise constantly, so making sure staff is on the current level regarding security policies and procedures is a part of securing IoMT. It is not expected that clinical staff be IT and cybersecurity experts, rather they must have a general understanding of HIPAA rules, the risk if ePHI is compromised, and the relevant security countermeasures they need to take to safeguard ePHI.

IoMT has many threats looking to exploit it, so having some knowledge of what adversaries are intending to do and what attacks can look like can reduce the likelihood of an attack or breach. Indeed, in the year 2019, 82% of healthcare organizations experienced a cyberattack on an IoT device [47]. The largest threat of these attacks was theft of patient data [47]. Theft of patient data can occur at many points in the IoMT environment. In the case of the LifeWatch MCT3L, patient data could be compromised if the sensor is lost or stolen, and the physical memory is accessed. There could also be MITM attacks during Bluetooth communication, intercepting the ECG data. In the Vivify Health RPM system, communications over an insecure WiFi network could be intercepted.

7.2 Lightweight Security Protocols for IoT

Lightweight security countermeasures are currently being developed to further protect information on resource constrained IoT devices. Glissa and Meddeb [30] propose a lightweight version of IPsec for IoT devices, called 6LowPsec, and end-to-end security solution for 6LowPan IoT devices. The purpose of 6LowPSec is to provide end-to-end security that reliably delivers time sensitive data in resource constrained environments while reducing overhead and computational requirements [30].

As mentioned earlier, there is a lack of end-to-end security in IoT devices, but the 6LowPsec protocol provides higher security for 6LowPan devices. 6LowPsec security features include data confidentiality and integrity through key association and management using AES-128. 6LowPsec also employs intrusion detection for advanced security [30]. The performance evaluation of 6LowPsec showed that it is an efficient protocol for 6Lowpan security. It replaces the need for upper layer security protocols while remaining lighter than IPsec. The lightweight encryption algorithm (LEA) for IoMT WBANs described by Alshamsi, et al. [42], encrypts biometric data gathered from a sensor before sending it to the mobile device. LEA is a block cipher that uses 128, 192, and 256 key sizes, the same as AES, but the number of rounds is 24, 28, and 32 [42]. The AES algorithm goes through 10 rounds for a 128-bit key, 12 for a 192-bit key, and 14 for a 256-bit key before the final encryption output is produced. The number of rounds is significantly higher for LEA, but the encryption round process is lighter. Indeed, LEA is approximately 1.5 to 2 times faster than AES [42]. Currently, there are also no known successful attacks on LEA [42] making it a highly secure and viable alternative to the mainstream AES algorithm. LEA is a solution for low power and resource constrained IoT devices that require confidentiality (e.g., the LifeWatch MCT3L sensor).

7.3 Technologies in Cloud Computing and Blockchain Used for IoT Security

An overview of the cloud for IoT was discussed in Chapter 2 Section 2.3, but the cloud for IoT truly shines as a security tool. The cloud can provide secure storage for IoT data in a private cloud, i.e., a cloud that is only accessible by authorized users. Mechanisms such as Amazon's Web Services simple storage service (S3) allows for scalable and secure storage of data. Any file can be stored in what's known as a bucket, a container for data [49]. AWS provides identity and access management to ensure safe storage of data. For example, public access to S3 buckets is automatically blocked by default [49]. In addition to secure storage, AWS also offers tools to monitor the activity of an S3 bucket [49]. AWS CloudTrail provides detailed logs of activity [49]. S3 is just one example of a solution for IoT data storage security. There are plenty of other cloud options available depending on need.

Blockchain technology is a unique system of data storage. Blockchain is a decentralized distributed ledger that secures data through cryptography and hashing algorithms [50]. Each node in a blockchain is signed with the previous block's hash, forming a peer-to-peer database [50]. Blockchains are decentralized because of the nature in which they store data and perform transactions; they do not require a third-party to verify the trust between blockchain nodes [50]. Trust between nodes is verified by all other nodes, i.e., every transaction in a blockchain is shared between every block [50].

For IoT, a blockchain can be a useful security measure in that it reduces the likelihood of a breach because of a third-party’s lack of security. All the information gathered from IoT devices can be cryptographically stored in a blockchain. In a setting where privacy is crucial, such as the medical field, a blockchain can provide the necessary security and privacy. The source of the transaction in a blockchain remains anonymous. The data in a blockchain is immune to change because each block relies on all previous blocks using hashing algorithms to secure the data [50].

Blockchains eliminate the need for an intermediary or third-party auditing to verify the data; blockchains are a self-sustaining secure database. Since IoT suffers from heterogeneity, blockchain provides a decentralized system for IoT devices that would otherwise have security issues in centralized storage. Adopting blockchains in IoT to manage the numerous transactions in IoT environments would also reduce the costs with maintaining a centralized data storage center [50]. Blockchains could be the next step to making IoT a universal seamless service.

One of the key issues with blockchains is that since it is a recent technology, there is a lack of regulations and guidelines [50]. This is important for manufacturers of IoT devices because they may need to meet certain criteria from regulatory bodies (e.g., the FDA) for approval. Another challenge of blockchains in the medical field is providing access of medical records to patients. A private blockchain would be necessary for healthcare and granting patients access to their medical records stored in a blockchain could be complicated. The blockchain would also have to comply with HIPAA rules for security and privacy.

Chapter 8. Conclusion

The purpose, architecture, and applications of IoT has been described and the implementation of real IoMT devices has been scrutinized. Key technologies such as Bluetooth and LTE were described as well as the threats and vulnerabilities of those standards. The main contributions of this thesis consist of the solutions to improve IoMT cybersecurity countermeasures and HIPAA compliance.

The two IoMT implementations examined in this thesis revealed important aspects of cybersecurity in IoMT. Both implementations examined lack critical cybersecurity countermeasures. There must be physical, technical, and administrative countermeasures to safeguard IoMT devices and ePHI. HIPAA rules apply to IoMT, and every covered entity must maintain compliance. IoT security must be improved if it is to remain the future of the internet. Future work may consist of examining advanced IoMT devices as the standards develop, as well as comparing the efficiency and security of new encryption methods to IoMT devices.

REFERENCES

1. Babu B., Srikanth K., Ramanjaneyulu T., Narayana I. "IoT for Healthcare." International Journal of Science and Research, volume 5 issue 2. February 2016.
2. Evans D. "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything." April 2011.
3. Al-Qaseemi S., Almulhim M., Almulhim H., Chaudhry S. "IoT Architecture Challenges and Issues: Lack of Standardization." Future Technologies Conference. 6-7 December 2016.
4. Foote, K. "A Brief History of the Internet of Things." https://www.dataversity.net/brief-history-internet-things/. 16 August 2016.
5. Gokhale, et al. "Introduction to IoT." International Advanced Research Journal in Science, Engineering and Technology ISO 3297:2007 Certified Vol. 5, Issue 1. January 2018.
6. Whitmore A., Agarwal A., Xu L. "The Internet of Things – A survey of topics and trends." Springer Science+Business Media New York. DOI 10.1007/sl0796-014-9489-2. 12 March 2014.
7. Von See A. "IoT Global Revenue 2019-2030." https://www.statista.com/statistics/1194709/iot-revenue-worldwide/. 19 October 2021.
8. "IoT Architecture: The Pathway from Physical Signals to Business Decisions." https://www.altexsoft.com/blog/iot-architecture-layers-components/. 12 August 2020.
9. Burhan M., Rehman R., Khan B., Kim B. "IoT Elements, Layered Architectures and Security Issues, A Comprehensive Survey." DOI: 10.3390/s18092796. 24 August 2018.

10. Gigli M., and Koo S. "Internet of Things: Services and Applications Categorization." *Advances in Internet of Things,* 2011, 1, 27-31. DOI: 10.4236/ait.2011.12004. July 2011.
11. Palavalli A., Karri D., Pasupuleti S. "Semantic Internet of Things." 2016 IEEE Tenth International Conference on Semantic Computing. DOI: 10.1109/ICSC.2016.35. 2016.
12. Lombardi, M., Pascale F., Santaniello D. "Internet of Things: A General Overview between Architectures, Protocols, and Applications." 19 February 2021.
13. Calihman A. "Architectures in the IoT Civilization." https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/#molongui-disabled-link. 30 January 2019.
14. Navani D., Jain S., Nehra M. "The Internet of Things (IoT): A Study of Architectural Elements." 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems. 2017. DOI 10.1109/SITIS.2017.8.
15. Xuyang L., Zhu P., Lam K.H., Zheng C. "Overview of Spintronic Sensors, internet of Things, and Smart Living." August 2016.
16. Kocakulak M., Butun I. "An Overview of Wireless Sensor Networks Towards Internet of Things."
17. Sable A. "Comparative Study on IEEE Standard of WPAN 802.15.1/ 3/ 4." *International Journal for Emerging Research in Science and Technology.* Vol1. Issue 1. June 2014.
18. Satybrata J. "Overview of Personal Area Network." https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/. 5 August 2021.
19. Leclair M. "Threats and Solutions to Wide Body Area Networks." https://www.l9group.com/research/threats-and-solutions-to-wide-body-area-networks. 25 September 2020.

20. Watts S., Raza M. “SaaS vs PaaS vs IaaS: What’s The Difference & How to Choose.” https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/. 15 June 2019.

21. Alsubaei F., Shiva S., Abuhussein A. “Security and Privacy in the Internet of Medical Things: taxonomy and Risk Assessment.” 2017 IEEE 42nd Conference on Local Computer Networks Workshops. DOI: 10.1109/LCN.Workshops.2017.72. 2017.

22. Nausheen F., Begum S. “Healthcare IoT: Benefits, Vulnerabilities, and Solutions.” 2018.

23. Yang L., Ge Y., Li W., Rao W. Shen W. “A Home Mobile Healthcare System for Wheelchair Users.” 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design. 2014.

24. Yang G., Xie L., Mantysalo M., Zhou X., Pang Z., Xu L., Kao-Walter S., Chen Q., Zheng L. “A Health Platform bases on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box.” IEEE Transactions on Industrial Informatics, Vol. 10 No. 4. November 2014.

25. Seh A., Zarour M., Alenezi M., Sarkar A., Agrawal A., Kumar R., Khan R. “Healthcare Data Breaches: Insights and Implications.” 13 May 2020.

26. Al-Masri E., Kalyanam K., Batts J., Kim J., Singh S., Vo T., Yan C. “Investigating Messaging Protocols for The Internet of Things (IoT).” DOI: 10.1109/ACCESS.2020.2993363. 2 June 2020.

27. Pala B. “What’s the Difference? UDP vs TCP.” 2 March 2020.

28. Tariq M., Khan M., Khan T.R.M., Kim D. “Enhancements and Challenges in CoAP – A Survey.” 9 November 2020.

29. “MQTT vs CoAP, the battle to become the best IoT protocol.”

https://www.pickdata.net/news/mqtt-vs-coap-best-iot-protocol. 21 October 2019.

30. Glissa G., and Meddeb A. “6LowPSec: An end-to-end security protocol for 6LoWPAN.” *Ad Hoc Networks.* Vol. 82. 2 February 2018.
31. Padgette J., bahr J. Batra M., Holtmann M., Smithbey R., Chen L., Scarfone K. “Guide to Bluetooth Security.” NIST Special Publication 800-121 Revision 2. May 2017.
32. Cichonski J., Frankilin J., Bartock M. ‘Guide to LTE Security.” NIST Special Publication 800-187. December 2017.
33. Chawla B., Gupta O.P., Sawhney B.K. “A Review on IPSec and SSL VPN.” *International Journal of Scientific & Engineering Research*. Vol. 5, Issue 11. November 2014.
34. Center for Disease Control and Prevention. “Health Insurance Portability and Accountability Act of 1996.” https://www.cdc.gov/phlp/publications/topic/hipaa.html.
35. American Medical Association. “HIPAA security rule & risk analysis.” https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis.
36. HIPAA Journal. “What is the HITECH Act?” https://www.hipaajournal.com/what-is-the-hitech-act/.
37. National Institute of Standards and Technology. “Guide for Conducting Risk Assessments.” NIST Special Publication 800-30. September 2012.
38. HIPAA Journal. ‘What are the Penalties for HIPAA Violations?” https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.
39. HIPAA Journal. ‘Ambulance Company Settles HIPAA Violation Case with OCR for $65,000.” https://www.hipaajournal.com/ambulance-company-settles-hipaa-violation-case-with-ocr-for-65000/.

40. BioTel Heart. “Patient User Guide LifeWatch Mobile Cardiac Telemetry 3 Lead.” 2020.

41. BioTel. “Quick Start Guide.” https://www.myheartmonitor.com/wp-content/uploads/sites/2/2019/06/SUP588-LifeWatch-Mobile-Cardiac-Telemetry-3-Lead-MCT-3L-Quick-Start-Guide-Rev-D-1.pdf.

42. Alshamsi A., Barka E., Serhani M. “Lightweight Encryption Algorithm in Wireless Body Area Networking for e-Health monitoring.” 2016 12th International Conference on Innovations in Information Technology. 2016.

43. Pai A. “UPMC leads $17M investment in Vivify Health for its remote patient monitoring system.” 25 February 2016.

44. Internet Engineering Task Force. “The OAuth 2.0 Authorization Framework.” https://datatracker.ietf.org/doc/html/rfc6749October 2012.

45. Anicas M. “An introduction to OAuth 2.” https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2. 21 July 2014.

46. Cawthra J., Grayson N., Hodges B., Kuruvilla J., Littlefield K., Snyder J., Wang S., Williams R., Zheng K. “Securing Telehealth Remote Patient Monitoring System.” NIST Special Publication 1800-30B. May 2021.

47. HIPAA Journal. “82% of Healthcare Organizations Have Experienced a Cyberattack on Their IoT Devices.” https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-a-cyberattack-on-their-iot-devices/. 3 September 2019.

48. Fagan M., Megas K., Scarfone K., Smith M. “Foundational Cybersecurity Activities for IoT Device Manufacturers.” NISTIR 8259. May 2020.

49. Amazon Web Services. “What is Amazon S3?”

https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html#S3Features. 2022.

50. Erdem A., Yildirim S., Angin P. “Blockchain for Ensuring Security, privacy, and trust in IoT Environments: The State of the Art.” (ed.) Mahmood Z. *Security, Privacy, and Trust in the IoT Environment.”* https://doi.org/10.1007/978-3-030-18075-1_3.2019.