AN INTRUSION DETECTION SYSTEM FOR INTERNET OF MEDICAL THINGS

by

Deborah Oladimeji

Submitted in partial fulfillment of the requirements
for the degree of Master of Computer Science

at

Dalhousie University
Halifax, Nova Scotia
June 2021

I dedicate this thesis to my amazing husband whose sacrificial care for me and our daughter made it possible for me to complete my entire program, my wonderful mother for her unconditional love and to my dearest daughter.

Contents

List of Tables

List of Figures

Abstract

The terms IoMT (Internet of Medical Things), IoHT (Internet of Health Things) and HIoT (Healthcare Internet of Things) are now all used interchangeably. They describe the connection of medical devices and software applications relating to healthcare information to the Internet using networking technologies. While these technologies bring the promise of improved patient care, improved efficiency, and reduced costs, they also bring new risks as many these connected devices are unmanaged and unprotected. The consequent potential impact is not just on patient data, but on patient care itself.

This thesis focuses on providing a highly secure transmission of medical data in IoMT to ensure accuracy and confidentiality of patients' data. We propose a novel intrusion detection system (IDS) based on machine learning (ML) methods which uses both network and biometric parameters as features and can differentiate the normal traffic from attack traffic. Six ML methods were selected for the intrusion detection, namely, Random Forest, K-Nearest Neighbor, Support Vector Machine, Artificial Neural Networks, J48 and Decision Table, and tested against man-in-the-middle and denial of service attacks using a dataset consisting of a combination of about 20,000 normal and attack healthcare data. The dataset was generated on our IoMT test bed that was implemented using four modules, namely, a multi-sensor board, a gateway module, a network module, and a visualization module. The communication between the modules employs a Client Server publish/subscribe messaging transport protocol, MQTT, which is a light weight, simple, easy to implement for constrained devices with limited resources, such as IoMT.

Experimental results indicate that our secured healthcare system can detect anomalies in both the network flow and patient's biometric readings. Furthermore, we generated a new healthcare dataset with the combination of biometric data and network traffic available for other researchers for statistical analysis and further research. Finally, we present a comparative summary of the proposed scheme with an existing scheme in terms of accuracy and execution time.

Acknowledgements

First and foremost, praises and thanks to **God Almighty** for His unending grace and showers of blessings to successfully complete my work.

My deepest and sincere gratitude goes to my research supervisor, **Prof. Srinivas Sampalli**. I am overwhelmed and humbled by his great support for me and the opportunity to work under his supervision. Your dedication, invaluable guidance and keen interest to help your students succeed have helped me accomplish this task.

Studying without funding might be extremely costly, but I am most thankful to my supervisor and **Dalhousie Faculty of Graduate Studies (FGS)** for the consideration for FGS Entrance Scholarship that has provided full financial support throughout my program, and turned my career dream into a reality.

I am extremely grateful to **Prof. Hiroyuki Ohno (Kanazawa University in Japan)**, for his exceptional support on the implementation of this project. His expertise, knowledge, and exacting attention to detail have improved this study innumerably.

I would like to express my gratitude to my special friend, **Darshana Upadhyay**, for her contribution throughout my MCS studies. Her valuable suggestions regarding this research greatly helped in completing this endeavour. Her encouragement and motivation have been a great inspiration to me.

I owe a deep sense of gratitude to all members of MyTech lab especially, **Sagarika, Wen,** and **Nupur**, for their support in the course of this research.

Finally, huge thanks to my greatest source of inspiration, my caring, loving and supportive husband, **Olaniyi**. What a great comfort and relief you gave by taking care of our daughter and managing the home. I am grateful to my adorable daughter **Olivia**, for her cooperation and for making nursing and studying enjoyable. Great thanks to family and friends, especially my **mother, mother-in-law** and my brother, **Sunday** whose love and guidance are with me always.

Chapter 1

Introduction

1.1 IoMT and Its Role in the Healthcare Sector

The advent of Internet of Medical Things (IoMT) has enhanced remote patient monitoring. It reduces unnecessary hospital visits and the burden on health care systems by connecting patients to their physicians and allowing the transfer of health data over a secure network. Healthcare professionals can monitor patients' key biometrics in real-time, access healthcare data in remote locations, and keep track of any potential issues that might occur, thus help preventing any future complications. IoMT has the potential to give more accurate diagnoses, less mistakes and lower costs of care through the assistance of technology, allowing patients to send health information data to doctors. Currently, this is essentially necessary due to the effect of the global pandemic, COVID-19, reducing in-person medical visits which prevents the spread.

IoMT has enhanced Remote Patient Monitoring (RPM) which helps in monitoring patients' vital signs such as heart activities and glucose level - the doctors can then be automatically alerted when necessary. IoMT can also help in triggering emergency responses and keep chronic diseases in check. For instance, wearables can help monitor heart rate and glucose levels. Those living in remote areas can share activity tracker information with a remote health provider with the use of smart devices and get a medically informed recommendation. IoMT has revolutionized the operations of health sector. For example, a report from Forbe [1] states "The Internet of Medical Things (IoMT) is poised to transform how we keep people safe and healthy especially as the demand for solutions to lower healthcare costs increase in the coming years".

IoMT has the potential for more accurate diagnoses, improved efficiency, improved patient care, and lower costs of care. It is capable of monitoring, informing and notifying not only care-givers, but also provide healthcare providers with specific data to help identify issues for earlier invention before they become critical [1]. IoMT helps insurance companies to view patient data more quickly and make the processing of claims faster and accurate. In fact, all stakeholders including the pharmaceuticals and insurance companies greatly benefit from IoMT due to improved quality of patient care.

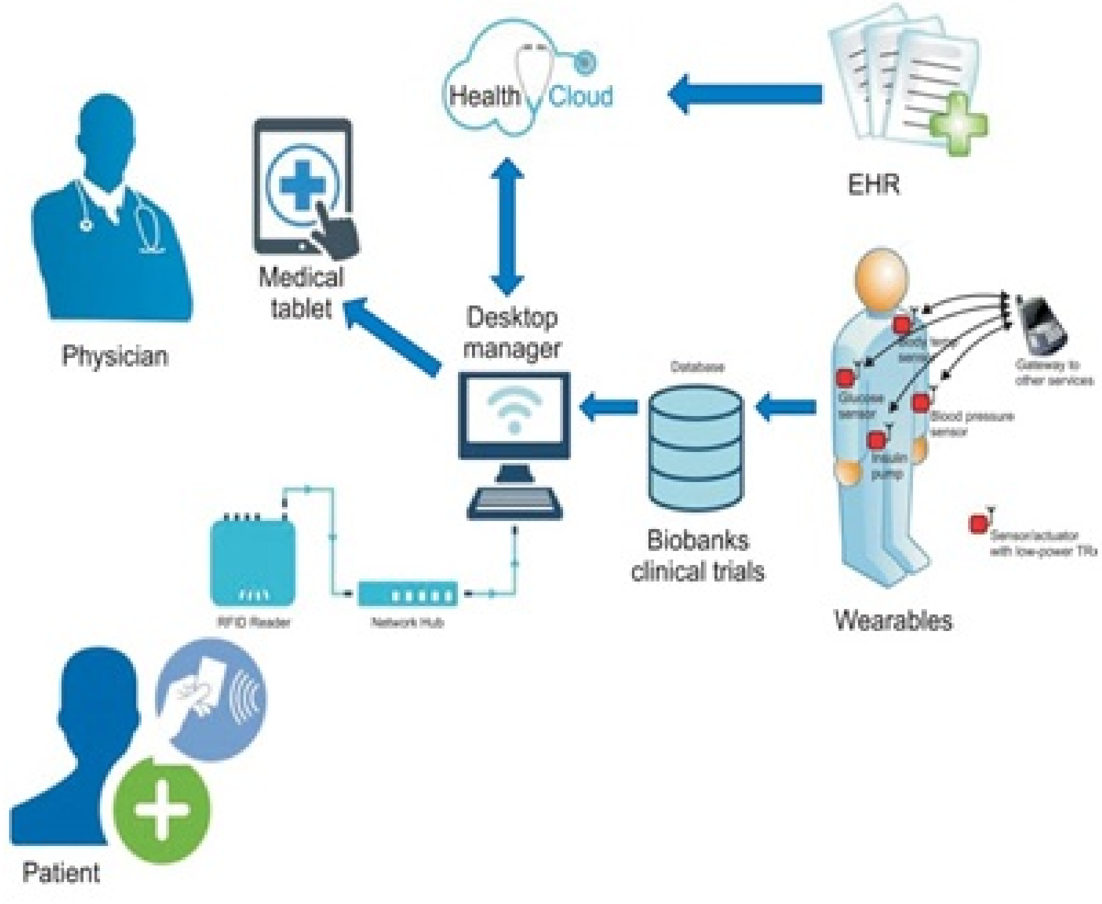


Figure 1.1: A typical IoMT System

According to Kamalanthan et al. [2], IoMTs are divided into 4 categories which are listed below:

1. Wearable devices: Smartwatches, temperature and pressure sensors, heart monitoring and muscle activity sensors, and glucose and biochemical sensors
2. Implantable devices: Swallowable camera capsule for visualization of the gastrointestinal tract, embedded cardiac pacemakers, and implantable cardioverter-defibrillators (ICD)

3. Ambient devices: Motion sensors, door sensors, vibration sensors, etc.
4. Stationary devices: Imaging devices like CT (Computerized Tomography) scan and surgical devices

Figure 1.1 shows the stakeholders and components in a typical IoMT system. IoMT can be considered to be a subset of Internet of Things (IoT) which comprises of smart devices, such as wearables and medical or vital monitors, tailored towards monitoring the health of people. Some of these wearables are smart devices that can monitor a user's physiological parameters such as oxygen saturation (pulse oximeter), blood glucose levels, heart rate, electrocardiogram (ECG) patterns, the electrical activity of cardiac pacemaker, etc., in real-time and transmit these data to the physician. It can be attached to the body, at home, or in community, clinic or hospital settings. The "Things," in the Internet of Medical Things, can refer to a wide variety of devices such as infusion pumps, heart monitoring implants, that are used to deliver a pre-programmed level of fluids into a patient. There are also numerous other devices such as insulin pumps, cochlear implants, and pacemakers. These devices collect and transmit data via the Internet to healthcare providers. It enables the healthcare providers to monitor a patient's health remotely. It also allows them to give timely response to issues when they happen, rather than waiting for patients to visit the physician in person. For example, someone who wears a smart health watch that tracks their heart rate and sleeping pattern; the tracker uses Bluetooth technology to tabulate the results on an iPhone; and then share that data with a physician to provide feedback via Wi-Fi connection. IoMT also include the connection of software applications that collect medical data that is provided to healthcare IT systems through online computer networks.

1.1.1 Security issues in IoMT

Not only is the Internet of medical things bringing positive changes to the healthcare sector, but also enabling a more human approach to care and healing. However, it is subject to a lot of cyber threats and vulnerabilities. Fasai et al. [3] highlighted the following as some of the reasons for high rate of cyber-attacks in IoMT: (1) Medical Things are primarily exchanging sensitive patient data. (2) Incompatibility and complexity arising from connection of huge number of devices and heterogeneous networks. (3) Being an emerging field, there is a high surge in embracing IoMT solutions without considering the security issues by the healthcare manufacturers. As a result, new security issues related to confidentiality, integrity, and availability (CIA) arise. (4) As most IoT components send and receive data wirelessly, this exposes IoMT to danger of wireless sensor network (WSN) security violations. (5) Application risks, such as breaches of authorization and authentication, as well as the overall security and availability of the application is also a major concern. (6) Some security computations consume considerable amount of computing resources. These are some of the main reasons that expose IoMTs to various malicious attacks.

Many of these connected devices are unprotected, and the potential impact is not just patient data, but patient care itself as any error in the data report or analysis of a patient could lead to their death. Therefore, it is of utmost importance to address how to identify and protect against attacks on medical devices. Most IoTs vulnerabilities are also applicable to IoMTs but some are more targeted towards IoMTs due to the sensitive nature of health data. These cyber-attacks include but not limited to data breach, MiTM(Man in The Middle) attack, replay attacks, and network communication decryption, Denial of Service(DoS) and security and privacy threats. Vulnerabilities in IoMT can be categorized based on the layer. Table 1.1. summarizes a 3-layer IoMT architecture with their corresponding cyber-attacks. Details of this can be found in [4] and [2]. An IBM study shows that healthcare organizations had the highest costs associated with data breaches [5]. Furthermore, according to Help Net Security, hackers breached Singapore's health service and stole personal information of 1.5 million patients, in addition to compromised outpatient medication data of 160,000 individuals, including Singapore's Prime Minister [6].

The healthcare industry is constantly afflicted by a myriad of cybersecurity-related issues. These issues range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care. The security of sensitive data such as protected health information that passes through the IoMT as well as uninterrupted access to the system is a developing concern for healthcare providers. While other critical infrastructure sectors experience these attacks as well, the nature of the healthcare sector's purpose poses unique challenges. It goes beyond financial loss and breach of privacy but has direct impact on human life. For whatever reason attack is being launched on the healthcare system, either large or small, they still pose a danger. As IoMT become an integral part of healthcare, we must find a way to manage them securely and effectively.

Table 1.1: Possible attacks at each 3-layer IoMT architecture

Layer	Description	Attacks
Application layer	This is responsible for delivering application specific services to the user.	Data Leakage, DoS attack, misconfiguration, SQL injection, account hijacking, ransomware, and brute force.
Network layer	The data that's collected by all of these devices are transmitted and processed by this layer.	Eavesdropping, replay, DoS attack, network injection, MitM.
Perception layer	This is characterised with the use of a number of digital devices that collect various amounts of data and request information from networks.	Device tampering, sensor tracking, Malicious code Injection.

We now highlight two major attacks on IoMT that are central to this thesis.

Man-in-the-Middle (MitM) Attacks in IoMT

A MitM attack occurs when an attacker intercepts communication between two systems either to secretly eavesdrop or modify the communication. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data. The attacker can disguise as the original sender that has the original communication and trick the recipient into thinking they are still getting a legitimate message. Within IoHT, we can imagine a scenario where a malicious party may want to fake vital readings sent from the patient monitor to the Central Monitoring Station (CMS) in other for the staff remotely monitoring a patient sees incorrect real-time information about vital readings. This is a dangerous attack in the health sector as the consequences might be life-threatening. Most of the medical devices send data either unencrypted or with weak encryption to the server which makes it more prone to MitM attacks.

Denial of Sevice (DoS) Attacks in IoMT

DoS attack on the other hand denies legitimate users from having access to the health system. This attack floods the smart devices with service requests, disrupting their availability. There are various forms of DoS attacks. It is used by cybercriminals to overwhelm a network to the point of inoperability. This can pose a serious problem for healthcare providers who need access to the network to provide proper patient care. Healthcare organization is one of the most essential sectors that need a consistent network uptime. This allows for Electronic Health Records (EHRs) to be accessed and life-critical applications to be run. As many of today's Internet of Medical Things (IoMT) devices are created with convenience and usability, it opens the door for attackers to target devices with DoS attacks that could knock entire organizations offline.

Downtime in the healthcare industry can be life-threatening. When DoS attacks knock networks offline, hospitals are unable to control IoMT devices, access electronic health records, conduct research, and more. There is need to ensure the healthcare system has a means of monitoring and scrutinizing all traffic flow in and out of network for easy detection of malicious event.

1.1.2 Machine Learning in Cybersecurity

According to Wikipedia, Machine learning (ML) is the study of computer algorithms that improve automatically through experience and by the use of data [7]. ML is typically considered as a branch of "Artificial Intelligence", which is closely related to computational statistics, data mining and analytics, data science, particularly focusing on making the computers to learn from data [8]. Using specialized algorithms with patient datasets can help medical professionals screen for diseases with a very high level of accuracy. An ML approach usually consists of two phases, namely, training and testing [9]. Often, class attributes (features) and classes from training data and, a subset of the attributes necessary for classification are identified, followed by the learning of model using training data, and the use of the trained model to classify the unknown data is performed [9]. Due to its versatility with big data, it is mostly used for data analysis in healthcare. ML technology has the ability to process more data faster automatically, making it a great compliment to any clinician's practice of medicine and a very efficient way of getting actionable data.

The healthcare industry is constantly dealing with huge amount of data from multiple different sources, and thus becomes highly essential to find a way of processing the data into useful information for clinicians. Machine learning can take disparate data from things like electronic health records, wearable devices, and lab testing and give physicians suggestions for care based on that analysis. This information can include diagnosis suggestions, disease risks, and pattern notifications in an increasingly accurate and efficient fashion. Combining its efficiency with the physician technical know-how, it serves as a clinical decision support to reduce the chance of errors.

Currently, machine learning in security is a fast-growing trend. The power of machine learning is harnessed in cybersecurity to better analyze threats and respond to attacks and security incidents. In a bid to improve malware detection, enterprise security vendors have been working towards incorporating machine learning into new and old products. Previous methods [9] used in detecting vulnerabilities like the "signature-based" system are now being upgraded to machine learning system that tries to interpret actions and events and learns from a variety of sources. With machine learning, cybersecurity systems can analyze patterns and learn from them to help prevent similar attacks in real time.

In this thesis, we used various machine learning algorithms to build an efficient Intrusion Detection System (IDS) for healthcare application using a variety of medical sensors. Intrusion detection is the process of dynamically monitoring events occurring in a computer system or network, analyzing them for signs of possible incidents and often interdicting the unauthorized access [10]. This is typically accomplished by automatically collecting information from a variety of systems and network sources, and then analyzing the information for possible security problems [11]. The system comprises of medical sensors from which data are generated, gateway for data gathering, an attacker system to launch attacks, an IDS to analyze flow of traffic for malware detection, and monitoring systems which receives health data for visualization. One of the monitoring systems, in addition to visualization purpose also serves as server to store all medical data. At this point, health data is made available for the medical practitioners. We applied ML methods for DoS and MitM attack detection.

We focus primarily on cyber intrusion detection as it applies to wired networks. However, the ML methods covered in this paper are fully applicable to the intrusion and misuse detection problems in both wired and wireless networks. The system indicates anomalies in the monitoring graphs to give alert during data manipulation and attempt to disrupt the network flow. This is done by analyzing both the patients' biometric data and network traffic vector. The system reports any threat if any anomalous behaviour is detected in any of the biometric data or network traffic feature. After thorough consideration of different ML methods to test the efficiency for security approaches, six ML methods were selected for the intrusion detection: Random Forest (RF), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Artificial Neural Networks (ANN), J48 and Decision Table. Random forest, like its name implies, consists of a large number of individual decision trees that operate as an ensemble. Each individual tree in the random forest outputs a class prediction and the class with the most votes becomes the model's prediction [12]. KNN is a ML model that classifies data points based on the points that are most similar to it [13]. Since this classifier relies on distance for classification, if the features represent different physical units or come in vastly different scales, then normalizing the training data can improve its accuracy dramatically [14]. SVM uses a hyperplane in an N-dimensional space to classify the data points [15]. N here is the number of features. ANN is a model that is inspired by the biological neural networks [16]. J48 is a decision tree classifier that uses a predictive machine-learning model which calculates the resultant value of a new sample based on various attribute values of the available data [17]. DT is a model used for specifying which actions to perform depending on given conditions [18]. For monitoring a patient, the ML-based methods will analyse the situation according to the trained dataset. The training dataset mostly plays an important role in the prediction of the future trend of a given new problem successfully [19].

1.2 Motivation

There is an old saying that "Health is wealth". In this scenario, in addition to health, health records are also wealth as adequate health services cannot be delivered without access to accurate health records. So it is more important to keep the medical records safe and secure. Access to efficient healthcare services is totally dependent on the correctness of the medical data as informed decisions are made from these. The emergence of IoMT, being an intensive data domain poses a major challenge in security aspect. There must be a way to secure a large amount of sensitive data without being tampered as it is estimated that there will be a significant increase in the utilization of IoMT platforms in the future. Also, given that health records have become a very valuable commodity, and the global coronavirus pandemic has created a slew of new opportunities due to the rise in telemedicine, it's not surprising to see a significant increase in healthcare cyber-attacks. Opportunistic hackers increasingly see medical records as flexible all-in-one identity theft packages and scam toolkits. Patients' lives will be at risk if no system is put in place to detect malicious event on the fly. Hence, there need to be an efficient technique to address this security issue. 82 percent of healthcare organizations had already been targeted by IoT device attacks in 2019 [20], before the insurgence of the global COVID pandemic which raises spike in cybercrime and escalated threats to IoMT devices. Given the implication of these threats on patients and the healthcare sector at large, improving cybersecurity protection for connected medical devices is not negotiable.

This research proposes an efficient intrusion detection system to secure a healthcare system for monitoring a patient. Without effective intrusion protection, any connected medical device – pacemakers, infusion pumps, vital signs monitors, smart pens, and more – is at risk of attack, whether it is connected to a hospital network or is one of the millions of distributed devices not connected to any network. Vital sign monitors generally come with poor encryption protocols for Bluetooth connectivity, raising the prospect that hackers could use these devices as entry points into health systems' networks, where they could steal patient data for financial gain. This jeopardizes the lives of the millions of patients who depend on them. With multiple IoMT devices connected to the hospital's network containing no security, they are bound to serve as the gateway of choice for hackers seeking the easiest way in. Entire hospital networks could then be infected with crippling ransomware. Many research initiatives tried to solve this important and timely problem but few works has considered the combined use of biometric readings and network traffic as a machine learning feature for detecting real time attack. MitM and DoS attacks could be devastating in any circumstance. Our design is able to spot both MitM and DoS attacks within seconds in the healthcare network, and report malware causing any interruption or damage to the healthcare network.

1.3 Thesis Objective

In recent years many extensive research has been performed in the security of IoMT area. Most of this research was focused on the use of signature-based, encryption techniques and cryptography protocols to improve authentication and integrity of the healthcare system. Gradually, the discussion was extended to the role of the Internet in improving the quality of medical services and the communication between patients, medical specialists, health providers and other authorities in the health system. Most of these works, however, are not much concerned about supporting the network with better service in terms of real time data availability to all specialists and immutability. Real time data availability implies the availability of medical data to all specialists at the same time at different or same location whether the specialist is connected to the hospital network or not. Immutability is the integrity of health data, which cannot be modified or altered. Furthermore, the evolution of IoMT technology has made it possible for people to gather information concerning their health status easily, anytime and anywhere using smart mobile devices. However, these medical data consist of personal private information that should not be susceptible to eavesdropping or malicious tampering during transmission, neither should the network be disrupted at any time. Therefore, the privacy protection, secure transmission and availability of electronic healthcare data has drawn more attention from many researchers. A secure and reliable healthcare framework to defend against hostile attacks is essential for informationalized healthcare industry. However, effective processing of the ever-growing volume of healthcare data simultaneously with the transmission of a secured health data remains a long-standing problem in healthcare research.

This thesis focuses on providing a highly secure transmission of medical data in IoMT to ensure accuracy and confidentiality of patients' data. We propose a novel Intrusion Detection System (IDS) based on Machine Learning (ML) methods which use both network and biometric parameters as features and can differentiate the normal traffic from attack traffic. Six ML methods were selected for the intrusion detection, namely, Random Forest, K-Nearest Neighbor, Support Vector Machine, Artificial Neural Networks, J48 and Decision Table, and tested against man-in-the-middle and denial of service attacks using a dataset consisting of a combination of about 20,000 normal and attack healthcare data. The dataset was generated on our IoMT test bed that was implemented using four modules, namely, a multi-sensor board, a gateway module, a network module, and a visualization module. The communication between the modules employs a Client Server publish/subscribe messaging transport protocol, MQTT, which is a light weight, simple, easy to implement for constrained devices with limited resources, such as IoMT.

Experimental results indicate that our secured healthcare system can detect anomalies in both the network flow and patient's biometric readings. Futhermore, we generated a new healthcare dataset with the combination of biometric data and network traffic available for other researchers for statistical analysis and further research. Finally, we present a comparative summary of the proposed scheme with an existing scheme in terms of accuracy and execution time.

1.4 Thesis Outline

The rest of the thesis is organized as follows: Chapter 2 provides the background. In this chapter, an overview of IoMT is discussed and different types of intrusion detection systems are introduces. Chapter 3 discusses recent research regarding this thesis. Chapter 4 describes the proposed intrusion detection system of IoMT, enumerating the research questions, methodologies employed to address the research problem, and the experimental environment. Chapter 5 focuses on describing the experimental results, discussion of the results, and comparison analysis with existing scheme. Finally, chapter 6 summarizes the contributions of this thesis, as well as areas of future research.

Chapter 2

Background

2.1 Overview of IoMT

2.1.1 IoMT Architecture

An IoMT architecture helps to better understand the composition of different layers in the system. There are several layers proposed in different papers with different terminologies for these layers. There is no single or general agreement about the architecture of IoMT that is agreed on by the researchers. Some researchers propose three layers while some support the four-layer architecture and some five-layer [21] as depicted in Figure 2.1. The enhancement in IoMT, the requirements of applications and the challenge in IoMT regarding security and privacy, are some of the major reasons behind the different architectures of IoMT. In this thesis, we have considered the three-layer architecture. These key layers are i) Application Layer, ii) Network or Transportation Layer, and iii) Physical or Perception Layer as shown in Figure 2.2. The smart applications of IoMT interconnected devices give personal as well as economic benefits to the society. Table 1.1 in chapter 1 summarized the different layers of IoMT system as well as the protocol stack, security issues and vulnerabilities of various underlying techniques.

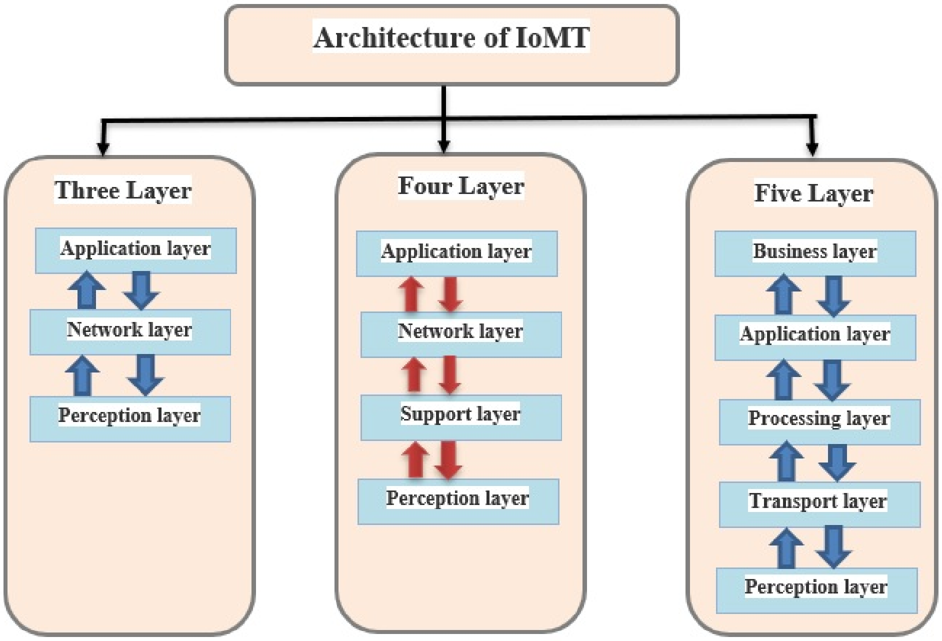


Figure 2.1: The layered architecture of IoMT (three, four, five layers)

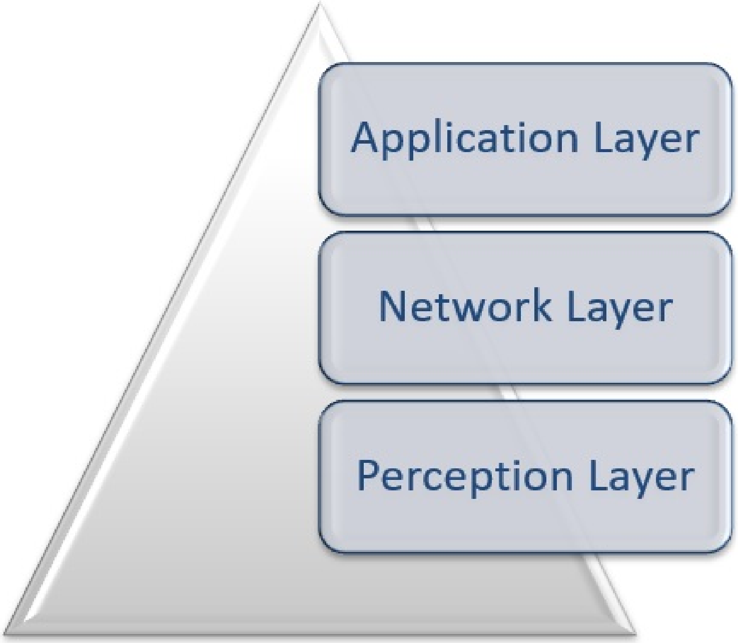


Figure 2.2: The 3-layer IoMT architecture

Application Layer

The topmost layer of the IoMT architecture is the application layer. This layer provides the personalized based services according to user relevant needs [22]. Its main responsibility is to link the major gap between the users and applications. This layer is implemented through a dedicated application at the device end. Similar to a browser on a computer implementing application layer protocols like HTTP, HTTPS, FTP, and SMTP, so also there are application layer protocols specified in context to IoMT as well. The application layer in the Internet is typically based on the HTTP protocol. However, HTTP is not suitable in resource constrained environment like IoMT because it is extremely heavyweight and thus incurs a large parsing overhead [23]. There are many alternate protocols that have been developed for IoT environments. Some of the popular IoMT application layer protocols include Message Queuing Telemetry Transport (MQTT), Secure Message Queue Telemetry Transport (SMQTT), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Representational State Transfer Hypertext Transfer Protocol (RESTful HTTP), Simple Object Access Protocol (SOAP), and Websocket. All the requests done from user is fulfilled here and this layer is known as the cloud layer [4]. The major concern of this layer is the privacy of data as heterogeneous devices are communicating with different IoMT standards. Different devices are exchanging the large amount of transaction of data and need to be secured [24]. It is responsible to provide all the required data to user requests and the major component for this data is privacy. Some data privacy techniques are also applied which include Transport Layer Security (TLS), Domain Name System (DNS), Secure Sockets Layer (SSL), etc [25]. Some of the protocols that provide data confidentiality, data authenticity and data integrity are CoAP, XMPP, Data Distribution Service (DDS) and web socket [26]. This layer includes any number of devices such as fitness/health system, monitoring system, remote diagnose system, tracking/locator system, medical e-record, telemedicine, etc.

Network Layer

The IoMT Network layer is responsible for routing packets from source nodes to destination and network addressing. It transmits and processes the data collected by all devices, and also connects these to other smart objects, servers, and network devices. The medium for the transmission can be wireless or wire based. The technologies used in this layer for IoMT are as Ethernet, wireless, 3G, LAN, Bluetooth, RFID, and NFC. Table 2.1 shows networking technologies used in IoMT. Ethernet connects stationary or fixed IoMT devices. IoMT uses Wi-Fi systems for connecting the gateway to the end-user as IoMT devices which can be stationary due to their continuous need for reliable power source [27]. Many IoMT devices with low power during their connection with end users and other nodes use radio spectrums like 3G, LTE and Bluetooth. For example, some medical devices in hospitals and clinics connect other devices with each other through Wi-Fi or low powered wireless personal area network (6LoWPAN) [28]. Bluetooth is widely used by wearables for short-range communications. The Bluetooth Low-Energy (BLE) standard was designed to meet the needs of low-power IoMT devices. It transfers only small portions of data and doesn't work for large files. ZigBee is a low-power wireless network for carrying small data packages over short distances. The outstanding thing about ZigBee is that it can handle up to 65,000 nodes [29]. It works effectively for IoMT devices due to its low-power capabilities.

Table 2.1: Networking Technologies used in IoMT

Network	Connectivity
Ethernet	Wired, Short-range
Wireless	Wireless, Short-range
3G	Wireless, wide-range
LAN	Wired/Wireless, Short-range
Bluetooth	Wireless, Short-range
RFID	Wireless, Short-range
ZigBee	Wireless, Short-range

Perception Layer

The main responsibility of this layer is data collection (i.e. heart rate, temperature, pressure, etc.) after which is transferred to the network layer. It is the physical layer which has sensors for sensing and gathering information about the environment. The perception layer is the lowest layer of the conventional architecture of IoMT. It senses some physical parameters or identifies other smart objects in the environment and transforms them into electrical signal. For instance, in the patient care systems, a number of sensors are connected to the patient's body to make sure that the patient's condition is being monitored. The description of some of the perception layer devices in IoMT is shown in Table 2.2.

Table 2.2: Description of Perception layer devices in IoMT

IoMT Device	Function
Activity Monitoring	Using gyroscope sensors for detecting patients' activities like (eating, sitting or sleeping).
Electronic Cardiogram	Assess the main functions of the heart for ensuring safety.
Temperatures Measurement	Providing results about body temperatures.
Biometric Sensor	Uniquely identify the patients' identity.
Locator	Tracing the patients' location.
Biochemical Sensors	Detecting biochemistry and harmful mixtures in the air.
Blood Pressure	Monitoring the patients' pressure.
Respiratory Rate	Monitoring the breathing rate.
Pulse Oximeters	Measuring both pulse and oxygen rate.
Heart Monitoring	Using both electrocardiography(ECG)) for monitoring the heartbeats.

2.1.2 IoMT Communication Technologies

The most common types of networks for IoMT applications technologies are Personal Area Networks (PANs), Local Area Networks (LANs), and Wide Area Networks (WANs). Each network type involves a number of wireless technologies, as shown in Table 2.3. In the following, we provide details of the architectures of IoMT communication environment. There are many communication technologies well known such as WiFi, ZigBee, Bluetooth, Li-Fi and LTE, but there are also several new emerging networking options. The choice of one or combination of communication technologies in IoMT is determined by the application, factors such as range, data requirements, security, power demands and battery life of the device.

Zigbee

ZigBee is a network protocol based on the IEEE.802.15.4 specification- a standard for low-rate wireless personal area networks (WPANs). It provides low-power consumption at a low cost to obtain the trust of maximum users [30]. It provides wireless communication to transmit information within a short range. It has a large installed base of operation, although perhaps traditionally more in industrial settings [31]. A Zigbee device typically has four layers—the IEEE.802.15.4 Radio, Zigbee Pro, Zigbee Cluster Library and Zigbee Certification. Zigbee Pro is the network infrastructure, implementing features ranging from communication band specification and pair mechanisms to security key generation and power saving. The Zigbee Cluster Library is the application layer, which is used to define clusters that are standard sets of messages/device behaviors to allow Zigbee devices to behave in a standard manner across devices [32]. This helps with interoperability, so Zigbee devices from different manufacturers can work with each other. Zigbee is capable of forming various arrangements of networks, or network topologies, between its devices. The most common network topologies are star, cluster tree, and mesh [32]. Each Zigbee network can consist of three types of devices: end device, router, and coordinator. A coordinator is responsible for creating the network as well as routing traffic through it. A network can only have one coordinator. A router is responsible for routing traffic, and an end device does not route traffic through the network. ZigBee has some significant advantages in complex systems offering low-power operation, high security, robustness and high scalability with high node counts as in healthcare and is well positioned to take advantage of wireless control and sensor networks M2M and IoMT applications. Its main advantage over another network protocol like WiFi is it's very low-power. This is a result of it being IEEE.802.15.4 standard plus the Zigbee protocol itself mandating lower power operation. While this does mean that Zigbee devices may not have a high range or push through much data, they do save power, money and maintenance work.

ZigBee provides security by assigning a network key to each of the device. Each device must have a network key assigned at the time of registration. A request is made for the network key when the device sends a request for communication. Therefore, only authorized and authentic devices can communicate to each other. It also has some disadvantages. The network key that is assigned can never be changed. It does not provide any facility to update or change the key, which is not a good tactic regarding security [30]. There are many applications of IoMT in which ZigBee technology is used like blood pressure monitor, pulse monitor, pulse oximeter, glucose meter and weight scale.

Bluetooth

Bluetooth is the IEEE 802.15.1 standard for low-power short distance radio frequency that can facilitate point-to-point and point-multipoint configurations, based on Wireless Personal Area Network (WPAN), which operates in the 2.4 GHz ISM band [33]. Bluetooth devices are cheap, and Bluetooth Low Energy (BTLE, BLE, or LE) (also called Bluetooth Smart or Version 4.0+) technology significantly reduces power consumption, and is a significant protocol for medical applications [34]. In addition to the similar Bluetooth range, it has been designed to offer significantly reduced power consumption.

Bluetooth is an important short-range communications technology, which has become very important in computing and many healthcare products. It is expected to be key for wearable products in particular, connecting to the IoMT probably via a smartphone in many cases. Bluetooth technology is well established and is able to provide wireless connectivity for an ever increasing number of IoMT devices requiring short range wireless connectivity. However, Smart/BLE is not really designed for file transfer and is more suitable for small chunks of data. It has a major advantage certainly in a more personal device context over many competing technologies given its widespread integration in smartphones and many other mobile devices [31]. Devices that employ Bluetooth Smart features incorporate the Bluetooth Core Specification Version 4.0 (or higher) with a combined basic-data-rate and low-energy core configuration for a RF transceiver, baseband and protocol stack. Importantly, version 4.2 via its Internet Protocol Support Profile will allow Bluetooth Smart sensors to access the Internet directly via 6LoWPAN connectivity [31]. This IP connectivity makes it possible to use existing IP infrastructure to manage Bluetooth Smart 'edge' devices.

Bluetooth provides many security mechanisms to ensure secure communication between sender and receiver. It provides a facility of encryption which converts a message into cipher text. On the other side, the receiver also has the ability to decrypt the cipher text into the original message. As a result of the encryption, the message can only be understood by the user who has the rights to see the message. It is mandatory for the sender to get permission from the receiver before sending the message. At first, the receiver receives a request which contains information the sender wants to share. It depends on the receiver to accept or reject the sender's request. There are many health monitoring devices in which Bluetooth technology is used like fitness and activity trackers, ECG, pulse, body temperature, etc.

Light-Fidelity (Li-Fi)

Li-Fi is a wireless optical networking technology that uses Light-Emitting Diodes (LEDs) for data transmission. The range of data transmission in Li-Fi is 100 times faster than Wi-Fi [35]. This is because Li-Fi is contained in a small area, and at that time, radio signals are spreading. It is optical, Visible Light Communication (VLC) system using light instead of radio waves in a manner similar to Wi-Fi [36]. VLC uses rapid pulses of visible light between 400 THz (780nm) and 800 THz (375 nm) for data transmission. Li-Fi uses transceiver-fitted LED lamps to transmit and receive information. Data are transmitted by the LED and received by photoreceptors, where the received signal is converted to the digital data [37]. The main idea behind Li-Fi technology is based on the production of very narrow pulses from the LEDs that are at very high frequency which cannot be detected by human eye however it can be sensed by a receiver. The component which is used to detect generated pulses can be a photodetector or a solar cell. The latter can be used alternatively as a power supply to the instrument and therefore can be combined to receive the signal as well as to power up the instrument.

Li-Fi allows transferring data to the network at speeds up to 1 GB / s, which means that it is 100 times faster than the speed of transfer to Wi-Fi. Growing demand for enhanced security, higher bandwidth, less emission, faster data streaming and low powered portable devices can extend the application of Li-Fi as data exchanging platform in the future. With the help of Li-Fi, the issues around spectrum and bandwidth might help overcome as more and more connected devices transfer critical data that can enhance decision making. In addition, the low price of a micro-LED lamp, combined with the power-saving capabilities, allows building a Li-Fi network to become cheaper and more energy efficient. Another advantage is that for an even distribution of the LED transmitter it is possible to get an internet connection much more accurately. It is accurate and stable inside buildings [38]. Li-Fi's advantages such as low cost and no room for eavesdropping since the signal does not travel through walls make it suitable for medical applications. Also, Li-Fi avoids the problem of overlapping frequencies known when using Wi-Fi for medical devices since there is no electromagnetic interference in VLC. Therefore, for example, Li-Fi can be used in a room to monitor patients while simultaneously radio waves are used for an MRI scanner [39].

Despite the numerous advantages Li-Fi offers, it has some drawbacks. It has network coverage and reliability issues. For instance, Li-Fi is unable to provide data in an area where there are walls, trees, or obstacles. Furthermore, the transmission path may cause disruption in the communication as a result of the interface from external light sources such as normal bulbs or sunlight. In addition, it is not possible to use Li-Fi technology in the existence of sunlight, or where there are mixed light media. In such environments, interference can cause weakening or disruption of light signals is formed, the light transmission is prevented, the light is weakened, which leads to a loss and loss of information at transfer.

Wi-Fi

Wi-Fi is a wireless communication network that transmits communication in the form of radio signals. Wi-Fi or 802.11, is a wireless protocol that was built with the main purpose to replace Ethernet using wireless communication. There are many Wi-Fi versions, such as IEEE 802.11x (Wireless LAN or WLAN), IEEE 802.11ac, IEEE 802.11n, IEEE 802.11g, IEEE 802.11a and IEEE 802.11b. Wi-Fi operates on three different non-interoperable technologies, which are Direct Sequence Spread Spectrum, Frequency Hopping Spread Spectrum (FHSS), and Infrared (IR) [40]. It has the ability to provide both point-to-point and point-multipoint configurations. It can use Multiple Input Multiple Output (MIMO) in order to maximize the use of the available bandwidth.

The latest Wi-Fi standard currently used in many applications is 802.11ac, which offers high throughput in the range of hundreds of megabit per second, which is fine for file transfers, but may be too power-consuming for many IoMT applications. Older Wi-Fi versions such as 802.11a, b, g and n are used in the healthcare field. Wi-Fi offers fast data transfer and the ability to handle high quantities of data. WiFi is uniquely placed to support broadband and narrowband IoMT applications from a common platform that can work at varying levels of power consumption and signal range. Its goal was to provide easy to implement, easy to use short-range wireless connectivity in addition to interoperability with devices from different vendors. Wi-Fi is able to support a diversity of connectivity in heterogeneous environments as found in IoMT as there will be a greater demand for machine-to machine (M2M) connections as IoMT gathers pace. Examples of IoMT with Wi-Fi technology are smart thermometer, connected inhaler, wearable biosensor, automation insulin delivery system, etc.

WiFi security can be provided by the following protocols [41]:

- **Wi-Fi Protected Access (WPA):** is a much stronger security protocol for Wi-Fi. It was introduced as an interim security enhancement over an older standard WEP (Wired Equivalent Privacy) while the 802.11i wireless security standard was being developed. There are two different modes of WPA. One of these WPA modes is used for Enterprises and the other is used for Individuals. These WPA Modes are Enterprise Mode (WPA-EAP) and Personal Mode (WPA-PSK). WPA-EAP uses an authentication server to generate keys or certificates. It is used with Extensible Authentication Protocol (EAP) and because of this it is more secured. WPA-PSK uses Pre shared and the implementation and management of this mode is easier. Although WPA is more secure than WEP, it was not enough. Different security vulnerabilities were detected on WPA [41].

- **Wi-Fi Protected Access II (WPA2):** It is the improved version of WPA, which includes the strong Advanced Encryption Standard (AES). WPA2 offered new encryption and authentication mechanisms to provide more secured networks. These mechanisms are AES and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). These mechanisms replaced the previous TKIP mechanism. TKIP is also used for interoperability, but as a fallback. WPA2 provides a sufficient security in the transmission of data [41].

Long Term Evolution (LTE)

LTE is an emerging wireless access network technology that has been considered the fourth generation (4G) wireless system to provide wide bandwidth access service to the Internet. . LTE provides UpLink (UL) data rate up to 75 Mbps, and DownLink (DL) up to 300 Mbps. It provides built-in security along with robust and scalable traffic management capabilities [42]. LTE is significantly more efficient than 2G or 3G which makes transporting data over a 4G LTE network to be done at a much lower cost per bit.

There are LTE chipsets and modules available today that have been designed to be flexible, efficient, and at low cost. Highly optimized for M2M and IoMT devices, these new solutions provide all the features and functionality required to build robust, long-life LTE devices for numerous applications at a low cost. Some of the features include ultra low power consumption, a small footprint, a mature and customizable software suite for easier integration, necessary for the many healthcare applications. It offers cost effective solution for M2M services for IoMT applications, including monitoring and tracking patients.

Long Term Evolution-Advanced (LTE-A)

LTE-A is the upgraded version of LTE, which increases the bandwidth, stability, and speed of traditional LTE networks. It uses MIMO (Multiple Input Multiple Output) technology to combine multiple antennas on both the transmitter and the receiver. Therefore, a 2x2 MIMO configuration would mean there were two antennas on the transmitter and two on the receiver. The more antennas there are the faster the speed can theoretically be, as the data streams can travel more efficiently [43]. This is then combined with ‘carrier aggregation’, which allows a device to receive multiple different 4G signals at once and they do not have to be on the same frequency. For instance, one could receive an 1800MHz and an 800MHz signal at the same time, which is impossible with the standard 4G.

It provides a scalable channel bandwidth up to 40 MHz, peak link spectral efficiency of 15 bit/s/Hz for downlink, and 6.75 bit/s/Hz for uplinks. LTE-A is interoperable with existing wireless standards and also gives room for multimedia support. In comparing with LTE network, it offers much faster peak speeds, for both downloads and uploads, as well as greater reliability, more seamless handover between networks, and global roaming. LTE-A technology is used in medical devices especially for remote monitoring devices.

5G

This is the fifth generation (5G) of wireless technology which promises more than just a faster network. It produces a redefinition of network, establishes a new global wireless standard for throughput, speed, and bandwidth. 5G is the successor of 4G and LTE-A technology. 5G can seamlessly connect a massive number of embedded sensors through the ability to scale down in data rates, power, and mobility, thus providing low-cost connectivity solutions.

5G networks can operate up to three frequency band which are low, medium, and high. Low-band 5G has a frequency range of 600–850 MHz, download speeds of 30–250 Mbps and range similar to 4G towers. Mid-band 5G uses a frequency of 2.5–3.7 GHz, speeds of 100–900 Mbps, with range of several kilometres. High-band 5G has frequency range of 25–39 GHz, download speeds in the Gbps range [44].

Table 2.3: Comparison of different Communication Technologies in IoMT

Technologies	Standard	Frequency	Range(m)	Data rates
Zigbee	IEEE 802.15.4	2.4Hz	10-100	250kbps
Bluetooth	IEEE 802.15.1	2.4Hz	50-150	1Mbps
Li-Fi	IEEE 802.15.7	>1MHz	<10	1̃Gpbs
Wi-Fi	IEEE 802.11	2.4 GHz & 5GHz	5̃0	600Mbps Max
LTE	3GPP	Depends on different number of band	Depends on different number of band	Uplink-75Mbps Downlink-300Mbps
LTE-A	3GPP	Depends on different number of band	Depends on different number of band	Uplink-1.5Gbs Downlink-3Gbs
5G	5G NR	Depends on different number of band	Depends on the frequency band	5̃0 Mbps to over a Gbps

2.1.3 Security Requirements in IoMT Communication Environment

Security is defined as a process by which unauthorized access to the system state is prevented and thus the privacy is not compromised. Security requirements consist of a set of traditional security requirements ensuring security of patients' information and system. It enables the users to protect and prevent IoMT-based healthcare system against known threats and attacks. In IoMT many sensor devices are connected with each other through Internet to provide healthcare services at anytime, anywhere, and any types of services. Although the majority of healthcare organizations do not spend enough resources to protect security and privacy, there is no doubt that security and privacy play a key role in IoMT. IoMT devices produce an increasingly large volume of increasingly diverse real-time data, which is highly sensitive. Destroying the security of medical network or system could be disastrous. Also, the patient's privacy information exists at all stages of data collection, data transmission, cloud storage, and data republication. Therefore, for secure IoMT, there must be a functional requirement that must be considered in the development. In the field of Information Technology (IT), three features are considered regarding security requirements. They are confidentiality, integrity, and availability, regarded as the prime objectives and are referred to as CIA triad [45]. These in addition to other requirements to meet the specific needs of IoMT environment is explained below.

Data Confidentiality

Data confidentiality assures protection of health information from being accessed by unauthorized parties. This is sometimes referred to as "privacy" which assures that the exchanged data in the channel should be protected against any kind of information disclosure attack. All relevant data being transmitted between communicating peers remains unknown for others. To prevent patients' health data from the leakage attack, such data needs to be kept confidential. This can be achieved using strong encryption schemes meaning that even if an adversary eavesdrops on transmitted packets, he cannot easily get access to them. Data confidentiality should also be resistant to any device compromise attack.

Data Integrity

Data integrity refers to a mechanism of ensuring that medical data is accurate and real. It means that the content of the received information does not contain unauthorised deletion, modification, and false insertion during communication. It ensures that patients' health data is received in the exact way as it was sent and it has not been manipulated in transit. Since most devices in IoMT systems interact wirelessly, maintaining data integrity is a necessary task. Health data need to be safeguarded against all forms of unauthorized modification. To provide data integrity, a Cyclic Redundancy Checksum (CRC), that is used to detect random errors during packet transmission, or a Message Authentication Code (MAC) are usually employed [46].

Data Availability

Data availability ensures all health data and devices are accessible to authorized users when needed. It means the continuity of services and prevention of any device failure and operational outage [47]. This is a very important need especially during treatment process, when timely patients' data should be available for physicians. Data must be available to users when needed for an efficient healthcare system. IoMT platforms must offer exceptionally high availability.

Authentication

Authentication validates the identity of the communicating parties or messages during the communication. Authentication allows the communication peers to ensure and validate the identity of each other before starting the secure communication. There is need for mutual authentication to be done in the entire system so that private medical information can only be accessed by authorized users. This way, an intruder cannot claim to be a valid user to obtain patients' medical data or inject invalid information. This can be achieved by sending a MAC (Media Access Control) along with the message. On the other hand, authorization indicates that only authorized users/sensors can access resources and services in an IoT-enabled healthcare system.

Information Privacy

Information privacy means that personal data and secretes of patients should not be disclosed without the consent [48]. IoMT system should be in accordance with privacy policies allowing the rightful owners to data, which are patients, control their private data. Patient information can be subdivided into two categories: general records and sensitive data. Sensitive data, which can also be called patient privacy, include mental status, sexual orientation, sexual functioning, infectious diseases, fertility status, drug addiction, and identity information. We need to ensure that the sensitive data is not leaked to unauthorized users, or even if data is intercepted, the information expressed cannot be understood by unauthorized users.

Data Freshness

Data freshness ensures freshness of information so that the previously exchanged health data should not be re-transmitted by an authorised party. It means that data should be recent ensuring that no old messages are replayed [49]. For example, physician needs to know the current patients vital signs information like his Blood Pressure (BP).

Scalability

Scalability refers to the capability of an IoMT device or system to continue functioning well even if such a system is subjected to modification in terms of size. For example, hardware, sensors, or services may be added or removed. In emergency situations, an IoMT should be capable of fast reaction without compromising the patients' security and privacy. It is necessary to minimize computation, communication, and memory overhead of medical sensors as a result of the low capabilities of these sensors. Hence, machine learning methods being used as IDS solution is recommended to fulfil the aforementioned requirements.

Access Control

In IoMT systems, caregivers (i.e. doctors, pharmacists, nurses, etc.) are directly involved with patients' medical and physiological data. Thus, a real-time access control needs to be available to restrict caregivers' access based on their privileges. After user identity verification, access rights to medical data should be determined so that different users can only access to the information required for on their tasks. For example, pharmacists should not have access to doctors' note apart from the drug prescription.

Mobility Support

Mobility support is one of the most important requirements in IoMT system which increases the applicability of these technologies. The mobility support enables patients to take a walk around the medical facility while he is continuously monitored. Also, mobility allows the patient to move from his base to other rooms for any medical tests without losing the continuous monitoring.

End-to-End Security

End-to-end security is one of the major requirements in IoMT system. It enables the end-points of a IoMT system, that is caregivers and medical sensors, to securely communicate with each other beyond the independent network.

Auditing

Auditing is the ability of a system to continuously track and monitor actions. In an IoMT system, there should be a record of all user activities in sequential orders such as login time to system and data modification time. Audit of health data access is an effective means to monitor the use of resources and a common measure for finding and tracking abnormal events. In addition, cloud service providers usually play untrusted roles, which require reasonable auditing methods.

Non-repudiation

Non-repudiation is a mechanism to ensure that someone cannot deny an action that has already been done. Non-repudiation assures that someone cannot deny the validity of something (i.e., message). It is widely used as an information security service which provides proof of the origin of message and the integrity of the data in that message. It makes it not too easy to successfully deny who or where a medical data came from as well as the authenticity of that data. Some of the mechanisms that offers non-repudiation is Digital signature.

Accountability

Accountability is one of the major requirements in IoMT. It ensures that an organization or individual is responsible for their actions. For example, in case of theft or abnormal event, the caregiver is obliged to be answerable for his actions.

2.1.4 Security attacks in IoMT devices

In IoMT, medical data are collected by connecting heterogeneous objects with different communication features in wired and wireless environments. All applications and systems serving the patients are prone to different kinds of security and privacy attacks. A huge amount of health data related to patient information, healthcare professionals, staff, hospitals, and also medical devices and equipment are gathered, analysed and stored. Today, health information is becoming digital as Electronic Health Record (EHR) is used whenever health information is to be shared across different health providers. This opens a huge number of privacy and security attacks. Protection of medical information for patient care and safety is a most important task. Ignorance of this issue will lead to an exponential rise in intrusion and might even end life. Most of the communication are wireless, which can makes spying extremely easy [50]. Potential opportunities of attacks increase with increase in number of IoMT devices. Healthcare facilities are particularly vulnerable to attacks due to improper layout of network. Unprotected data may be destroyed, modified or stolen or subject to any form of attack. Therefore, in order to ensure the high level of medical data security in the process of collection and processing, it is necessary to take precautions by knowing the threats and weaknesses in IoMT environments.

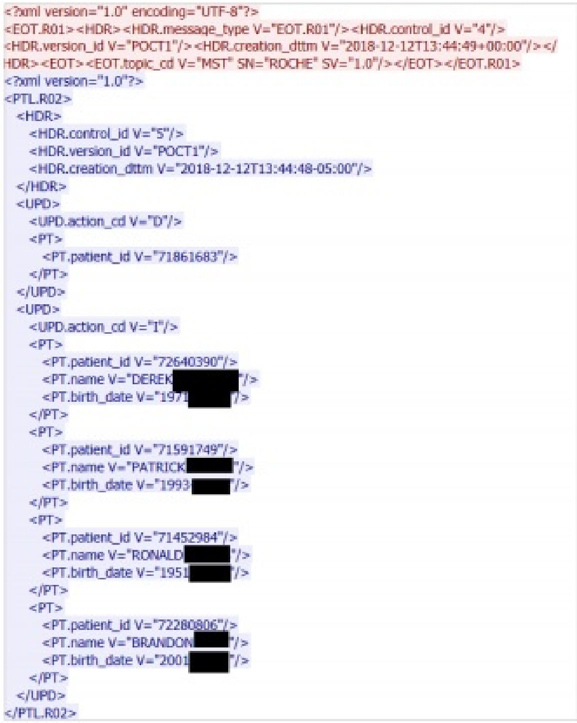
2.1.4.1 Types of attacks

Today, attackers are getting creative with their tactics and are finding new ways to hack into these devices to cause a security breach. Some of the various threats on connected devices in IoMT include eavesdropping - an attacker intercepts a patient's data during transmission, jamming - an attack launched by simply emitting an interference signal to block the communication on a wireless channel, brute force - use of hard-coded logins with the hope of eventually getting the correct login details, ransomware - sensitive data are encrypted and decryption is done in exchange for money, replay - reuse of an authenticating message that was previously exchanged between legitimate users, Cross-Site request forgery (CSRF) - attack to trick the end user into acting on a vulnerable application without the user's knowledge. session hijacking - attacker takes over the the session data of session connection at the web interface level and controls it, Cross-site scripting (XSS) - injecting malicious code to bypass access controls through web pages, SQL injection - execution of malicious SQL statements to bypass the devices security measures so as to read, alter or modify data from database management system (DBMS), side channel - taking advantage of information leakage to steal patient data by monitoring electromagnetic activity around specific medical devices, account hijacking - intercepting the communication performed between IoMT components while an end user is being authenticated, tag cloning - duplicating data gathered from a successful side-channel attack to access unauthorized data, tampering devices - physical tampering with sensors to partially or entirely stop or manipulate their functionality, and rogue access - installation of a forged gateway within the wireless network range that allows a user access.

As discussed earlier, DoS and MitM attacks pose a serious problem in IoMT network as transmission of medical data is intercepted or access to the system is denied. Efficient schemes must be designed to protect against this attacks to ensure that healthcare networks remain operational.

2.1.5 Insecure protocols

In this section, we describe the insecure medical protocols used in IoMT devices. These are some of the standard medical protocols developed by vendors for use in healthcare organizations to transmit data over the network. Research as shown that some of these protocols are insecure and are still in use in many health facilities [51]. These medical protocols often lack authentication and encryption, or they do not enforce its usage. Some of these protocols are HL7 (Health Level Seven), DICOM (Digital Imaging and Communications in Medicine) and POCT01 (Point-of-Care Testing). HL7 standard defines a format for the transmission of health-related information [52]. DICOM is the international standard for medical images and related information information [53]. POCT01 is a framework used to connect the devices to various information systems in healthcare facilities especially for laboratory testing devices [54]. These standards cite the possibility of encrypting transmitted data in their standardization documents [51]. This gives rooms for attackers to tamper, sniff and inject malicious traffic into the network. However, in healthcare networks the potential consequences are much more severe, since the data being transmitted is very sensitive, and the effects of tampering with commands issued by these devices can result in loss of life. For example, Figure 2.3 [51] shows POCT01 traffic containing personal data of patients, coming from a Roche Accu-Chek glucose monitor.



```
<?xml version="1.0" encoding="UTF-8"?>
<EOT.R01><HDR><HDR.message_type V="EOT.R01"/><HDR.control_id V="4"/>
<HDR.version_id V="POCT1"/><HDR.creation_dttm V="2018-12-12T13:44:49+00:00"/></
HDR><EOT><EOT.topic_cd V="MST" SN="ROCHE" SV="1.0"/></EOT></EOT.R01>
<?xml version="1.0"?>
<PTL.R02>
  <HDR>
    <HDR.control_id V="5"/>
    <HDR.version_id V="POCT1"/>
    <HDR.creation_dttm V="2018-12-12T13:44:48-05:00"/>
  </HDR>
  <UPD>
    <UPD.action_cd V="D"/>
    <PT>
      <PT.patient_id V="71861683"/>
    </PT>
  </UPD>
  <UPD>
    <UPD.action_cd V="I"/>
    <PT>
      <PT.patient_id V="72640390"/>
      <PT.name V="DEREK[redacted]"/>
      <PT.birth_date V="197[redacted]"/>
    </PT>
    <PT>
      <PT.patient_id V="71591749"/>
      <PT.name V="PATRICK[redacted]"/>
      <PT.birth_date V="1993[redacted]"/>
    </PT>
    <PT>
      <PT.patient_id V="71452984"/>
      <PT.name V="RONALD[redacted]"/>
      <PT.birth_date V="195[redacted]"/>
    </PT>
    <PT>
      <PT.patient_id V="72280806"/>
      <PT.name V="BRANDON[redacted]"/>
      <PT.birth_date V="200[redacted]"/>
    </PT>
  </UPD>
</PTL.R02>
```

Figure 2.3: Patient data in clear text (POCT01 Protocol)

2.2 Intrusion Detection Systems

An Intrusion Detection System (IDS) is a software application used to monitor a single or a network of computers for malicious activities aimed at spying information, stealing or corrupting network protocols. It defends and detects and various devices (for example, smart medical devices) from the possible attacks. Any malicious activity or violation is typically reported or collected centrally using a security information and event management system. The main purpose of an IDS is to inform the network administrator of a network intrusion that may be taking place. Information of alert will generally include details about the source address of the intrusion, the target address, and type of attack suspected. IDS in an IoMT environment monitors and verifies all traffic, both normal and malicious, and detects the possibility of malicious signs. If any malicious activity is detected, the application sends information to the administrators or block the of malicious IP address of that source. In IoMT environment, devices may stop working or may work in an inappropriate manner under the influence of an attack, for example, an implanted smart pacemaker can give shock to a patient which may become the reason of his death, hence, the protection of the IoMT communication environment from intrusion becomes necessary. As an active safeguard technology, IDS can provide the real-time protection for internal attacking, external attacking and misoperation.

Most techniques used in today's IDS are not able to deal with the dynamic and complex nature of cyber attacks on IoMT. Hence, efficient adaptive methods like various techniques of machine learning can result in higher detection rates, lower false alarm rates and reasonable computation and communication costs. In this paper, we used several machine learning methods and compare their performance. The following are the functions of an IDS [55]:

- Identification of sign of an intrusion.
- Provision of information about the location (i.e., suspected IP address) of the intruder.
- Logging of the information of ongoing activities.
- Stopping of detected malicious activities.
- Reports the information of malicious activities to the administrator.
- Provision of information about types of the intrusion.

2.2.1 IDS Detection Types

There are different classifications of IDS but the common ones are Network Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). This classification is based on their deployment location.

Network Intrusion Detection Systems (NIDS)

NIDS monitors network traffic for particular network segments or devices and analyzes the network and application of protocol activity to identify suspicious activity [56]. It has visibility into all traffic flowing through the network and makes determinations based upon packet metadata and contents. This wider viewpoint provides more context and the ability to detect widespread threats. However, these systems lack visibility into the internals of the endpoints that they protect. A NIDS is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network [57]. Example of a NIDS is using snort over a network

Host-based Intrusion Detection Systems (HIDS)

A host-based IDS is deployed on a specific endpoint and it is designed to protect it against internal and external threats. It runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. The advantage a HIDS has over a NIDS is that it may be able to detect malicious network packets that originate from inside the organization that a NIDS has failed to detect. Also, it may be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems [57]. Such an IDS may have the ability to monitor network traffic to and from the machine, observe running processes, and inspecting the system's logs. A host-based IDS's visibility is limited to its host machine, decreasing the available context for decision-making, but has deep visibility into the internal of the host computer.

Furthermore, an IDS mechanism can be divided into three categories: a) anomaly based detection, b) misuse based detection, and c) specification based detection [55].

A. Anomaly based detection

Anomaly detection systems detect network activities different from normal system behaviours. This approach looks for runtime features that are out of the ordinary. Anomaly based intrusion detection monitors network traffic and compares it against an established model to determine whether it can be considered as normal for the network with respect to protocols, ports, bandwidth, and other devices [57]. All future behaviour is compared to this model, and any anomalies are labelled as potential threats and generate alerts. Anomaly detection has some techniques such as mobile agent based, statistics, data mining, neural networks. It often uses machine learning to establish a baseline and accompanying security policy. By detecting threats using a broad model instead of specific signatures and attributes, the anomaly-based detection method improves upon the limitations of signature-based methods, especially in detecting novel threats. Anomaly detection works well for unknown attacks but sometimes its false alert rate can be high.

The baseline used by this approach for comparism can be defined with respect to the history of the test signal (unsupervised) or with respect to a collection of training data (semi-supervised). Some authors refer to training data as a 'signature'. Semi-supervised approaches train with a set of truth data while unsupervised train with live data. Researchers take different approaches for discrete, continuous and multivariate data sets. Examples of a discrete data set are dialed numbers or system state. Example of a continuous data set is position and data rate. An example of a multivariate data set is a 3-tuple of position. The main advantage of anomaly based approaches is that they do not look for something specific. This eliminates the need to fully specify all known attack vectors and keep this attack dictionary current. One major disadvantage is the susceptibility to false positives. While this approach can detect novel or zero-day threats, the difficulty of building an accurate model of "normal" behaviour means that these systems must balance false positives (incorrect alerts) with false negatives (missed detections) [58]. Another major disadvantage of this category is that the system is vulnerable during the training phase. A feature is a component of a multivariate data set (e.g., data source, data sink, position start time and end time,). The size of the feature set is a coarse indicator of efficiency for anomaly based approaches; larger feature sets suggest a larger memory requirement and higher microprocessor use.

B. Misuse based detection

Misuse Detection technique, also known as Signature based detection, use known attack signatures. It looks for runtime features that match a specific pattern of misbehaviour. Signature-based IDS solutions use fingerprints of known threats to identify them. Once malware or other malicious content has been identified, a signature is generated and added to the list used by the IDS solution to test incoming content. This enables an IDS to achieve a high threat detection rate with low false positives because all alerts are generated based upon detection of known-malicious content. This detection system has a knowledge base including signatures of known attacks and weak points of the system. However, a signature-based IDS is limited to detecting known threats and is blind to zero-day vulnerabilities. Misuse Detection is very successful to detect known attacks but it's drawback is straining for new unknown attacks [59].

These approaches only react to known bad behaviour. The theoretical hypothesis is that a good node will not exhibit the attack signature. The key disadvantage of this type is that the techniques must look for a specific pattern which means a dictionary must specify each attack vector and remain updated. An attack signature can be a univariate data sequence, for example, bytes transmitted on a network. One sophistication is to combine simple data sequences into a multivariate data sequence [58]. An important research problem in this field is creating an effective attack dictionary. Signature length is a coarse indicator of efficiency for signature based approaches. Longer signatures suggest a larger memory requirement and higher microprocessor use. Signature based approaches are more effective against outsider attacks.

C. Specification based detection

Specification based intrusion detection looks for abnormal behaviour at the system level, and then compare it with anomaly based intrusion detection that analyzes specific user profiles or data flows. Specification based intrusion detection approaches formally define legitimate behaviour and indicate an intrusion when the system departs from this model. It has the capability to detect the unknown attacks. It utilises the advantages of both anomaly and misuse based detection approaches by using manually defined specifications and constraints to diagnose the abnormal behaviour. Basically, this approach is similar to anomaly based detection as it detects the attacks on the basis of deviation from the normal behaviour. At the same time, it works on the basis of manually defined set of constraints and specifications. One major advantage is a low false negative rate. Only situations that violate what has been previously defined by human expert as proper system behaviour generate detections. Another major advantage of specification based intrusion detection is the system is immediately effective because there is no training phase. However, the major drawback of this mechanism is the high time consumption and effort required to generate a formal specification. Specification based intrusion detection approaches are especially effective against insider attacks as they focus on system disruption [58]. On the other hand, they are not the best approach for outside attackers because the specification (e.g., state machine or grammar) is application-specific and pertains to actions that only an insider can take.

Chapter 3

Literature Review

This chapter discusses the details of security protocols used in IoMT communication environment. The literature review can be categorized into 5 major categories based on the security approaches as follows; 1) Encryption and Cryptography based approaches, 2) Access control based approaches, 3) Authentication based approaches, 4) Blockchain based approaches, and 5) Intrusion detection based approaches.

3.1 Encryption and Cryptography

Linzhi et al. [60] propose an efficient Scheme for Homomorphic Evaluation (SHE) over Single Instruction Multiple Data (SMID) to realize remote auxiliary Medical Diagnosis (MD) while protecting confidentiality of the medical data and ensuring patients' privacy (PP). They implemented a new set of efficient SIMD homomorphic comparison and division schemes. Based on the findings, they implemented efficient privacy preserving and SIMD homomorphic surf and multiretina-image matching schemes. Delivered functionalities include SIMD homomorphic feature point detection, multiretina-image matching, and lesion detection for the encrypted retinal image of diabetic retinopathy. They provide a proof-of-concept application implementation toward remote auxiliary diagnosis systems for diabetes in order to showcase the core security and privacy pillars of the solution. The encryption scheme is based on lattice, which is quantum-resistant, and can preserve data confidentiality for quantum computation. Security and privacy requirements of the system is provided by using quantum-resistant homomorphic encryption scheme on patients' retinal images of diabetic retinopathy before being transmitted and stored at different devices to provide data confidentiality.

Haiping et al. [61] propose a key distribution scheme based on a Group Send–Receive Model (GSRM) and advanced encryption standard (AES) in the design of a healthcare system (HES) framework that collects medical data from WBANs, transmits them through an extensive wireless sensor network infrastructure, and publishes them into wireless personal-area networks via a gateway. The HES involves the groups of send-receive model scheme to realize key distribution and secure data transmission. The homomorphic encryption based on matrix scheme is used to ensure privacy, and an expert system able to analyze the scrambled medical data and feedback the results automatically is employed. Theoretical and experimental evaluations are conducted to demonstrate the security, privacy, and improved performance of HES compared with current systems or schemes. Security of medical data transmission in wireless sensor networks is provided by key distribution schemes and block encryption methods. A reasonable key distribution scheme is capable of improving the efficiency by decreasing the resource consumption of computation, memory, and communication of sensors. The security analysis of the system is carried out and it is protected from the following attacks; leakage of privacy, Eavesdrop attack, Chosen plaintext attack, Replay attacks, and Camouflage trust attack.

Jinquan et al. [62] propose a secure energy-saving communication and encrypted storage model by adding secure energy-saving communication scheme and encryption algorithm to the traditional medical cloud model. It focuses on the security and energy consumption of medical Electronic Health Record (EHR) data transmission and storage between cloud server and IoT device users. The communication authentication scheme is an algorithm based on elliptic curve and bilinear pair. In the algorithm, the two communication peers can complete the key establishment and identity authentication only after one communication, which effectively balances the resource overhead of the key center and the user, and resists the Man-in-the-middle attacks and password cracking. The algorithm maintains the Rivest Cipher 4 (RC4) encryption efficiency, reduces the amount of cipher text data, and also improves confidentiality, randomness and security of the key stream. In view of the characteristics of large amount of medical data and high repetition rate, Huffman compression algorithm is combined with RC4 to reduce the cipher text size while maintaining the encryption efficiency. Comprehensive analysis and simulations show that the system is secure, energy-saving and highly efficient for EHR. The architecture of system model can be divided into 3 layers. The bottom layer includes EHR users, medical IoT devices, attackers and medical institutions. The middle layer is the key infrastructure where user's basic information in EHR and the information collected through IoT device are encrypted and uploaded to the medical cloud server through RC4 algorithm. The system is also secure against weak key attack, key collision attack and brute force attack.

Neha et al. [63] propose a Blockchain Enabled Authentication Key Management Protocol for IoMT environment, called BAKMP-IoMT. BAKMP-IoMT provides secure key management between implantable medical devices and personal servers and between personal servers and cloud servers. The legitimate users can also access the healthcare data from the cloud servers in a secure way. Blockchain technology is employed to store all the healthcare data and maintained by the cloud servers. A detailed formal security including the security verification of BAKMP-IoMT using the widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is performed to demonstrate its resilience against the different types of possible attack such as replay attack, MitM attack, impersonation attack, Ephemeral Secret Leakage (ESL) attack, and privileged-insider attack. In order to improve the security of BAKMP-IoMT, three factors are used for authentication purpose: 1) mobile device of a user which stores significant credentials required for authentication, 2) password of user , and 3) personal biometric of user. Different random nonces (numbers) and current timestamps are utilized to safeguard against replay attack. All the network entities participating in BoMT communication environment are assumed to be synchronized with their clocks. Cryptographic one-way hash function and bitwise XOR operations is utilized to form BAKMP-IoMT lightweight as IoMTs are resource constraint in nature. Fuzzy extractor is utilized at the user side for biometric verification. Expensive computations are carried on resource-rich devices such as user's mobile device and cloud server in order to provide better security in the network. The comparison of BAKMP-IoMT with existing related schemes shows that the proposed system provides better functionality and security, in addition to low communication and computational costs needs.

3.2 Access control

Jinesh et al. [64] proposed an Enhanced Context-aware Capability based Access Control (ECCAPAC) model to make the medical network to be resilient against crypto attacks. The authors considered trust value of the object based on relevance and node importance to enhance the context information. Their main idea of the scheme is that access control is done based on the capability tag with capability and context information. In the proposed scheme, trust value is evaluated from the relevance and node importance factor is added for the context value in the capability tag. The model is dynamic, and the decision is based on a trust context. They compared the scheme with Role-based (RBAC) model and analysis shows that the approach achieves the resiliency against eavesdropping attack, MitM attack, key control attack, and replay attack.

Yang et al. [65] proposed a Lightweight Break-glass Access ontrol (LiBAC) system that supports two ways to access encrypted medical files: attribute-based access and break-glass access. Access to the data is granted in normal situations if a medical worker with an attribute set satisfying the access policy of a medical file, while during emergency, access to medical data by making the break-glass access mechanism bypasses the access policy of the medical file. The scheme uses two access control modes: attribute-based access mode and break-glass access mode. In attribute-based access mode, legitimate data users decrypt and access patient's medical records with their attribute secret keys. The break-glass access mode is used during emergency situation, whereby an Emergency Contact Person (ECP) utilizes the password to extract the break-glass key, and decrypts the medical records to save patient's life. The authors argued that the medical records are secure since they are indistinguishable against chosen plaintext attacks, and that the break-glass key generation and extraction algorithms leak no information about the password and break-glass key.

3.3 Authentication

Bakkiam et al. [66] proposed an authentic-based preservation protocol to resolve the privacy preservation issues in the IoMT. They have a designed a Secure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS) in ensuring there is a secure communication in healthcare applications. The scheme is composed of three phases which are user registration, system login, authentication and revocation/reissue. It uses three communication entities namely medical expert, wireless gateway access and medical sensor. The user registration phase chooses a user identity that imprints a biometric template to store user authentication parameter into smartcard. The system login and authentication phase carries out login phase for user and authenticate all entities such as wireless gateway access and medical sensor. The revocation or reissue phase performs the periodical revocation of the smart card at a cyclic basis. They showed that the scheme is resilient to withstand potential attacks such as privileged-insider attack, stolen smartcard attack, stolen-verifier attack, known-key attack, gateway-forgery attack etc. The authors also proved that an intruder cannot impersonate as a legitimate user to illegally access or revoke the smart handheld card. They have also provided a performance analysis to show that the proposed scheme provides high-security features to build smart healthcare application systems in the IoMT.

Vidyadhar et al. [67] proposed an authentication centric multilayered security model to provide a generic security framework for healthcare applications. The 2-way authentication centric multilayered security architecture is performed using authentication and key generation phase. The scheme features its heterogeneous set of users to interact with the token-based resource accessing environment in healthcare scenario, preventing unauthorized users accessing the personalized medical devices. The authors implemented the security model in cloud level which offers the secured access to both device and cloud-based healthcare application. It comprises of two phases namely phase 1 and phase 2. In the first phase, the user generates a login request from a common interface with allowed attributes and successful authentication of user and will return to the consequent session with the Session Key. In the second phase, user generates a resource access token with the issued session key. Then, user ID is generated and context is embedded with the validated user ID. Upon successful validation of user, policy is generated with an attribute and hence, permission is dispensed out along with the user roles and responsibility. The proposed authorization model invokes the capability dependent context-aware access control mechanism, offering multilayered protection for accessing healthcare resources. It uses Policy descriptor to assign the capabilities to each user according to their respective roles. Also, rules are defined by the policy descriptor such that the user is designated to issue commands (e.g., POST, GET, etc.) to medical resources in whichever the way he is entitled to do. The authors have demonstrated that context-aware capability based controlled access mechanism can be employed in securing medical devices in an energy efficient way.

Debiao et al. [68] proposed a new anonymous authentication scheme for keeping data's confidentiality and preserving patients' privacy. Their scheme consists of three algorithms which are initialization, registration and authentication. They have considered three participants in the network model such as the WBAN client, the Network Manager, and the Application Provider. The WBAN client is a user who could access the WBAN through a smart phone as, the Network Manager denotes a trusted third party that generates system parameters and users' secret keys, while the application provider is a remote system such as servers and medical systems at a hospital, or physician's medical office responsible for providing medical. Firstly, network manager generates the systems parameters and the Application Provider's public/secret keys. Second, WBAN client gets his private key by registering with Network Manager. Finally, WBAN client and Application Provider could authenticate each other. Previous anonymous authentication scheme saves data in Application Provider's database for verification purposes which the authors proved that it is prone to physical engineering attacks such as firmware modification and parameter tampering in memory. Therefore, they have saved generated security credentials in Network Manager for verification purposes and argued that it is the right approach to enhance the security of the healthcare system.

3.4 Blockchain

Recently, Blockchain is evolving as one of the most promising and creative technologies for security but also comes with its drawbacks which will be discussed later in this section. Mohammed and Khalid [69] proposed a blockchain based scheme to secure the Internet of Medical Things. The proposed approach consists of four components namely cloud server, network cluster, medical facility, and smart medical devices. The authors combined Elliptic Curve Cryptography (ECC) with Identity-Based Credential (IBC) to provide a key establishment mechanism for IoMT devices. They also introduced the bolster, which hosts the local blockchain in each medical facility. Each medical facility contains a powerful computing device called bolster that operates as a gateway/server to support in-range smart medical devices. The bolster holds a private and secure block role. The scheme uses it to provide securely communication with other blocks in the same blockchain. Their experimental analysis shows that the proposed scheme provides promising results towards a highly secured and privacy preserving IoMT.

Asaph et al. [70] proposed a decentralized record management system to handle Electronic Medical Records (EMRs), using blockchain technology. The system gives patients a comprehensive, immutable log and easy access to their medical information across providers and clinic sites. It leverages on blockchain properties to manage authentication, confidentiality, accountability and data sharing. The model integrates with providers' existing, local data storage solutions to facilitate interoperability. The authors incentivize medical stakeholders such as researchers and public health authorities to participate in the network as blockchain miners. This gives them access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. They have used smart contract on an Ethereum blockchain to automate and track some transitions log. They also used it to log patient-provider relationships that associate a medical record with viewing permissions and data retrieval instructions for execution on external databases. They incorporated a cryptographic hash of the record on the blockchain to protect against tampering, which guarantees data integrity. Patients can authorize sharing of their medical records between providers. The authors addressed identity confirmation using public key cryptography and employ a DNS-like implementation to map an already existing and widely accepted form of ID to the person's Ethereum address. They implemented a syncing algorithm to perform data exchange between a patient database and a provider database, after referencing the blockchain to confirm permissions via their database authentication server.

Vaggelis et al. [71] proposed blockchain-enabled authorization framework for providing secure interaction between patients, doctors, health-care personnel and device manufacturers in IoMT devices. Their main goal is to control the access of users to medical data and devices. The authors created a distributed chain of custody and health data privacy scheme by building trust domains for the various stakeholders and IoMT devices, such that legitimate users is enabled a fine-grain access. They have used a private blockchain in combination with on-chain smart contracts to allow for a forensics-by-design management architecture with audit trails for integrity and provenance guarantees as well as health data privacy. The private blockchain ecosystem is authenticated by a proof-of-medical-stake consensus mechanism that is tailored for medical applications. The smart contracts provide fine-grain authorization, carry out system policies and enforce transaction log integrity and privacy. The architecture assures build-in forensics since the blockchain provides a tamper-proof record of transactions. A consensus proof of medical stake validates the transactions. The authors informally examine the security and privacy assurances of the proposed blockchain-enabled authorization frame to prove its efficiency for securing healthcare management systems.

3.5 Intrusion Detection

Geethapriya et al. [72] develop a novel mobile agent based intrusion detection system to secure the network of connected medical devices. In particular, the proposed system is hierarchical, autonomous, and employs machine learning and regression algorithms to detect network level intrusions as well as anomalies in sensor data. They simulated a hospital network topology and perform detailed experiments for various subsets of Internet of Medical things including wireless body area networks and other connected medical devices. At the data acquisition layer, wearable systems such as wireless body area networks, smart and connected things such as smart bed as well as traditional diagnostic systems such as MRI, ultrasound were used to monitor, collect and relay the data to local gateway nodes or cluster heads, and perform data processing, aggregation and/or provide distributed storage. WBAN communication with cluster head/gateway device was done using IEEE 802.15.6 standard. Smart beds and other connected medical devices (MRI, ultrasound) connect either using wired or wireless communication to the hospital network. The sensors used in wireless body area networks include wearable or implantable sensors, placed in and around patients' body. The authors showed through simulation results that they were able to achieve high detection accuracy with minimal resource overhead. Although, mobile agent based intrusion detection systems reduce network traffic, provides ease of deployment and resiliency but security is a major challenge of mobile agents.

Asmae et al. [73] proposed an Intrusion Detection System based on the network parameters to identify jamming attacks in WBAN. The proposed solution is designed to detect three types of jamming which are Constant jammer, Reactive jammer and Deceptive jammer. The authors divided the concept of detection of attack into two main phases namely the initialization and monitoring step. The initialization of the scheme consists of calculating the thresholds of the network parameters Packet Delivery Ratio (PDR), Bad Packet Ratio (BPR), Received Signal Strength Indication (RSSI) and Energy Consumption Amount (ECA) of each receiver medical sensor. The assumption is that the WBAN system is operating normally in this phase without jamming attack. In the second phase, each sensor node monitors periodically its parameters, by comparing the initial (PDRth, BPRth, RSSIth and ECAth) and current values, in order to observe any problem. For constant jamming, the input values of PDR and BPR parameters are very lower than their thresholds values since most of packet data are damaged. Deceptive jamming is present when the input value of sensor is very low to the PDRth value, but the BPR, RSSI and ECA parameters is higher to their threshold. On the other hand, in the case of reactive jamming, the ECA value is still normal due to the fact that this type disrupts the communication when the legitimate send the packet RTS, and the jammer node does not wait for the packet SIFS (Short Inter Frame Spacing), which makes BPR and RSSI values to be higher compared to the input values of sensor while the PDR value is very low. They argued that the proposed IDS technique is able to differentiate the normal state and abnormal state as false alerts from jamming state. However, because it was simulated in Castalia platform, validation might not be ascertained until implementation is done with medical sensors.

Anar et al. [74] built a real-time Enhanced Healthcare Monitoring System (EHMS) testbed that monitors the patients' biometrics and collects network flow metrics. The monitored data is sent to a remote server for further diagnostic and treatment decisions. Man-in-the-middle cyber-attacks have been used, and a dataset of more than 16 thousand records of normal and attack healthcare data was created. The system then applies different machine learning methods for training and testing the dataset against these attacks. The EHMS testbed system works by first collecting data from the sensors attached to the patient's body across the network. It goes through the gateway to the switch and finally to the display screen of the server. An attacker is set to intrude while the data move from the switch to the server, to spoof or alter data before its reaches the server. The IDS computer is set to capture both Network and patient data metrics, which is then processed at the IDS for training and testing the machine learning methods as well as real-time detection of any abnormalities. The system uses Argus to collect all network traffic flows and patient data between the gateway and the server. The security of transferred data in the testbed is provided by the use of ML to monitor the healthcare in order to detect any tampering in the transmitted data between the nodes in the network in real-time. The system reports a threat alert to the system managers if any intrusion is detected. Both network flow packets and the sensed data from the sensors attached to the patient's body are used to train the model. The proposed technique is similar to our proposed architecture with the use of both biometric and network parameters. Their system however is limited to detect only MiTM attack. They have also argued that ANN gives the optimal model for securing the healthcare system which we proved not to be efficient in our model. Comparison analyses are provided in this paper.

Chapter 4

Proposed Intrusion Detection System of IoMT

This chapter describes in detail the proposed technique. The research questions addressed by this thesis are first enumerated, followed by the discussion of the research problem. The proposed technique makes use of machine learning models to detect intrusion in IoMT networks; as a method for providing both security, management and achieving secure communication among different medical stakeholders.

4.1 Research Questions

The most important research question addressed by the thesis is that of whether using both network flow metrics and biometric data as feature in ML models gives more promising result compared to when only one of the two types of features is used. Another important related question is whether healthcare information can be provided securely to medical experts/practitioners.

4.2 Research Problem

The above approaches for securing and providing intrusion detection and prevention in IoMT comes with several limitations like encryption and cryptography based approaches, authentication, access control mechanism, and blockchain based approaches have several limitations in fully protecting healthcare networks and systems from increasingly sophisticated attacks like denial of service. Not all encryption and cryptography based approaches can be directly applied to the healthcare system, especially when considering resource constraints and the requirements of the expert system. In addition to this, it raises challenges such as heavy overhead. Current symmetric key cryptographic algorithms, such as the Advance Encryption Standard (AES) used to ensure data confidentiality are indeed very secure. Similarly, asymmetric algorithm for digital signature and key exchange (Rivest Shamir

Adelman (RSA)) is also very secure. Secure Hash Algorithms (SHA) provides data integrity, Diffie Hellman (DH) is used for key agreement, Elliptic Curve Cryptography (ECC) provides an efficient asymmetric cryptographic techniques. Although all the aforementioned algorithms are very secure and effective, they require more CPU power and consume more battery power. These algorithms are therefore not feasible to use for securing IoMT.

The emerging blockchain technology is capable of potentially addressing the security and privacy issues in IoMT. Blockchain can provide IoMT with some security protection when integrated with other security mechanisms such as asymmetric cryptographic schemes and digital signature. Also, the decentralization of blockchain systems also mitigates the risks of the failures due to single-point-failure and malicious attacks. Blockchain also has intrinsic features such as traceability and immutability, which can further improve the data integrity of IoMT. However, blockchain's complexity, including high computing costs and delays, is a big challenge in the integration of blockchain with IoMTs that have restricted power and storage capacities. The high computational power required to run Blockchain algorithms has slowed down the advancement of these technology-based applications on resource constrained devices. Also, blockchain throughput is limited to meet the need of continuously generated streams of data in IoMT systems.

Most healthcare systems built on IDS techniques suffer from high false positive and false negative detection rates and the lack of continuously adapting to changing malicious behaviors. Recently, however, several ML techniques have been applied to the problem of intrusion detection with the hope of improving detection rates and adaptability. Our work focuses on providing a more efficient attack detection rate with low false positive and false negative detection in IoMT systems.

It is evident that although, several security architectures have been proposed to address security issues in IoMTs, the focus of most of the architectures is mainly on providing encryption and authentication in these systems. The smaller size of some medical devices and their limited memory and computational capabilities often hinders the use of cryptographic security solutions in IoMT. In addition, while encryption and authentication approaches provide reasonable defense to outsider attacks, they are often not capable of defending the network from insider attacks.

When a legitimate node in the network that has the cryptographic keys is compromised, it opens up a breach in the network wide security breach through a range of insider attacks within the network. There is a need for a second line of defence which can be provided by Intrusion Detection Systems, when legitimate nodes in the network are compromised.

Having discussed various measures for detecting intrusion and providing security in IoMT, we describe our proposed IDS that is based on ML models and the network parameters and biometric features as indicators for detecting MitM and DoS attacks.

4.3 Methodology

4.3.1 Enhanced IDS for IoMT

Our testbed has been built using medical sensors attached to the patient's body. We consider a typical architecture of connected medical devices in a hospital networking environment as shown in Figure 4.1. The data acquisition layer in this system consists healthcare monitoring sensors such as temperature sensor, blood oxygen saturation sensor etc. The sensors in the IoMT network include electrocardiogram (ECG or EKG) sensor, Blood Oxygen Saturation (SpO2) sensor, temperature sensor and blood pressure sensor, placed in and around patients' body. These sensors are attached to a multisensor board via each of their wire connector. These sensor nodes monitor, collect and relay the data to local gateway nodes through the multi-sensor board. The multi-sensor board is connected to a Windows-based computer using a USB port. It also has the capability of connecting via the Bluetooth. MQTT protocol has been used to collect data from the multisensor board. The Windows computer serves as a gateway from which data is transferred to the monitoring systems. This is done through Wi-Fi using TCP/IP protocol. The data is being sent to the cloud via MQTT publish and subscribe feature through which all other monitoring systems connect using the MQTT client. The monitoring systems could be the medical practitioners computers. Only the gateway computer connects wirelessly, the rest of the machines are connected to a switch using Ethernet cables. The switch is then connected to the internet through a router and the gateway computer makes internet connection via Wi-Fi.

ML techniques are used to detect any tampering in the transmitted data in the healthcare monitoring system in real-time. Upon detection, the system sends report to the system administrator. Also, medical practitioners can view reports on their systems. Both the network flow packets and the biometric readings from the medical sensors attached to the patient's body are used to train the model. The data is assumed to be transmitted in plain text as other encryption methods require more processing power, which is generally not achievable with low-power sensors.

Our proposed design is shown in Figure 4.1, as seen in the flowchart shown in Figure 4.2, data flows from the medical sensors attached to patient's body through the multisensor board to the gateway, switch and lastly, to the server and other monitoring systems for visualization. While the data travels from the gateway to the server, an attacker may modify the medical data before getting to the server or launch DoS attacks to stop the data from reaching the visualization stage. Meanwhile, network flow and patient biometric data metrics are captured at the IDS computer. The captured data is processed at the IDS for training and testing the machine learning methods for real-time detection of any anormalities. Our system uses Wireshark to capture network traffic and Argus to extract useful flow metrics, while it uses "cu" [75] and "awk" [76] command to collect all biometric data from the multisensor board. All monitoring systems get data by subscribing to the MQTT topic.

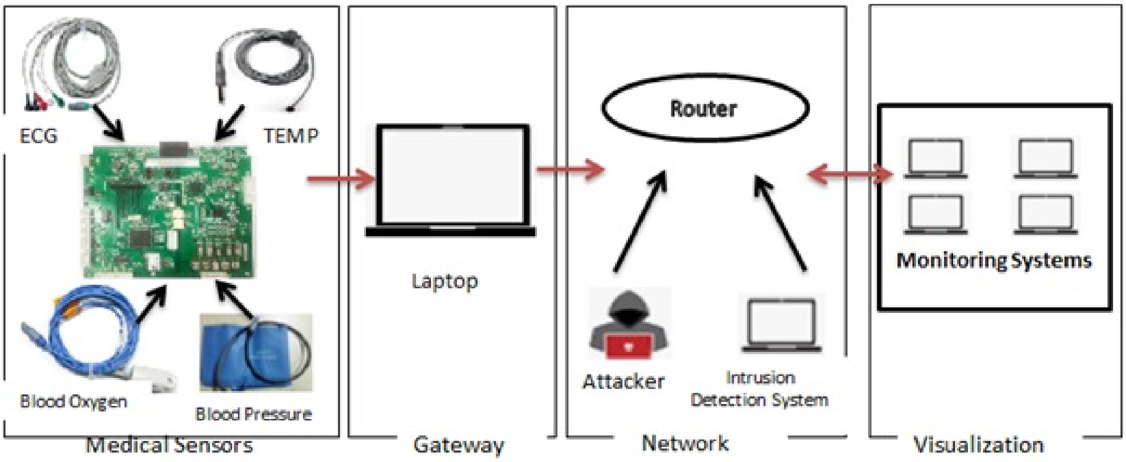


Figure 4.1: A Secured Healthcare Monitoring System

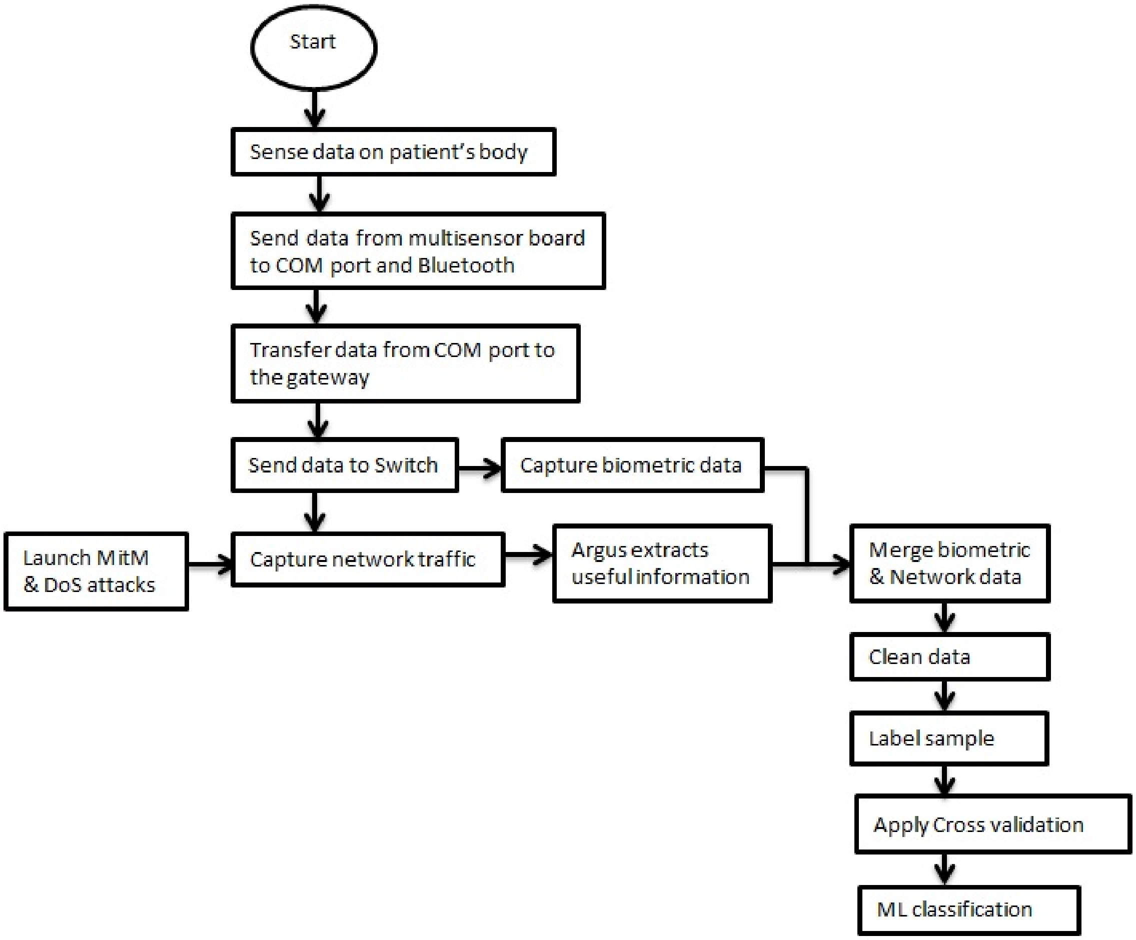

Start
Sense data on patient's body
Send data from multisensor board to COM port and Bluetooth
Transfer data from COM port to the gateway
Send data to Switch
Capture biometric data
Launch MitM & DoS attacks
Capture network traffic
Argus extracts useful information
Merge biometric & Network data
Clean data
Label sample
Apply Cross validation
ML classification

Figure 4.2: IDS Flowchart

4.3.2 Attack Model

In this section, we describe the attacks the system uses to carry out the intrusion process in the healthcare system. Both MitM and DoS attacks are implemented in the system.

MitM Attacks

The attacker pretends to be a legitimate user and connects to the router. The attacker gets the data first before it travels to the monitoring systems. Figure 4.3. depicts the structure of a MitM attack.

Data Modification/Insertion: The medical data get modified by inserting a pseudo data before getting to the monitoring systems. A bash script, "data_gen.sh" is run automatically to insert and modify patient's biometric data. In data modification attack, the attacker computationally fabricates invalid data that is not related to any physical phenomena observed by body sensors. It disrupts the system by tricking the health care providers to continuously respond to false alarms. This type of attack is fairly easy to execute in IoMTs.

```
$ bash ~/data_gen.sh | mosquitto_pub -l -t deborah/test1
-h broker.hivemq.com -I clientId
```

Data/Privacy Breach: The attacker gets unauthorized access to private medical information which violates the privacy and confidentiality required in healthcare systems. Since the attacker connects to the router, it routes all private data to its computer. This can be a medium for blackmail or for financial gain. Medical institutions could also be forced to make payments to avoid facing disciplinary action from certain health regulation bodies.

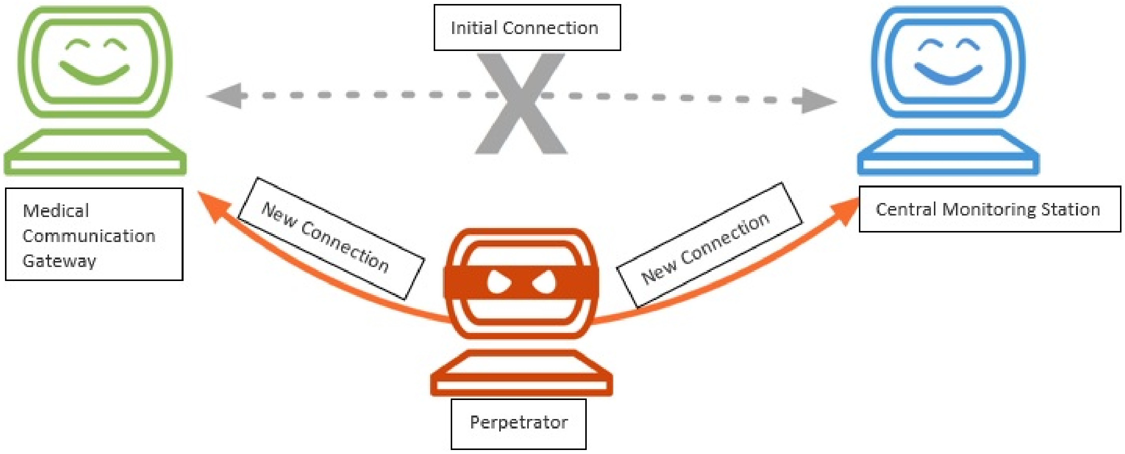


Figure 4.3: Man-in-the-Middle attack in IoMT

DoS Attacks

We consider our attacker to possess the ability to hijack and overwhelm the IoMT network to the point of inoperability. We model this attack in such a way that an adversary is interested in endangering a patient's life for ransom benefits by ensuring the healthcare providers do not receive emergency alerts when necessary. DoS attacks generally overwhelm the network, consume significant bandwidth and result in a denial of service to legitimate users. This can pose a serious problem for healthcare providers who need access to the medical information to provide proper patient care.

DoS attacks is launched through several methods as described below using Hyeane software:

Address Resolution Protocol (ARP) Request: This attack involves sending malicious ARP packets to the router in order to change the pairings in its IP to MAC address table. The attacker continuously sends a false ARP reply message, informing it that his MAC address should be associated with his target's IP address. As a result, the attacker blocks communications to the legitimate MAC address. It is very easy to carry out since the attacker has direct access to the network.

Internet Control Message Protocol (ICMP) Echo: This is a common DoS attack in which the attacker overwhelms the healthcare network with ICMP echo requests also known as a Ping. Usually, ICMP echo-request and echo-reply messages are used to ping a network device in order to diagnose the connectivity of the device and the connection between the sender and the device. The attacker send ping floods to the router in order to disrupt communications between computers on the IoMT network. By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the other legitimate users to become inaccessible to medical information.

TCP SYN: This attack floods the healthcare system with SYN requests in order to overwhelm the router and make it unable to respond to new real connection requests. It drives all of the router server's communications ports into a half-open state. Unlike other types of DoS attacks, it is not intended to use up all of the router's memory, but rather, to exhaust the reserve of open connections connected to a port. With SYN flood attack, the attacker sends TCP connection requests faster than the router can process them, causing network saturation. The intruder continuously sends SYN messages until the router reaches its half-open-connection limit and can't respond to any new incoming requests.

User Datagram Protocol (UDP) Flood: In this attack, a large number of UDP packets are sent to the router with the aim of overwhelming the router's ability to process and respond to request. The cumulative effect of being bombarded by such a flood is that the healthcare system becomes overwhelmed and therefore unresponsive to legitimate traffic.

4.4 Experimental Environment

In this section, we describe our experimental setup, attack models and assessment metrics. We simulate Internet of Medical things that consists of heterogeneous devices communicating using different network protocols. We consider a combination of wireless sensing devices using either bluetooth or the Ethernet standard. To address the communication protocol disparity, we ensure the proposed system is designed to be compactible to different network standards. Figure 4.4 shows all medical sensors connected to the PM6750 multisensor board. Our system consists of four major building blocks: a multi-sensor board, a gateway, a network and visualization phase. The functionality of each block is explained below:

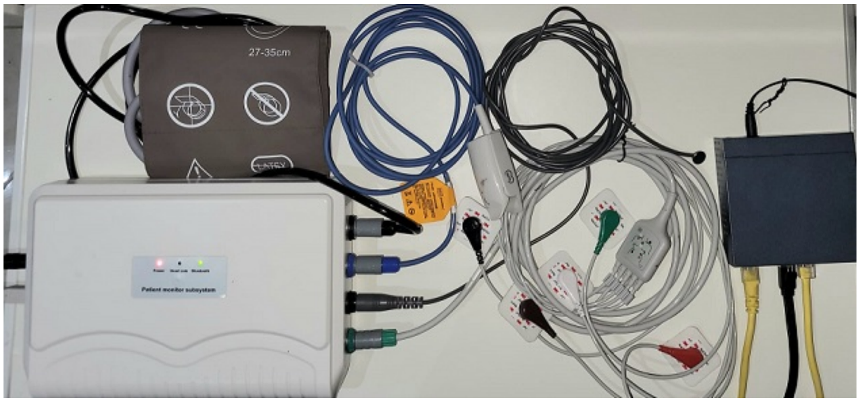


Figure 4.4: Connection of module PM6750 to all medical sensors

PM6750 Patient monitor Multi-sensor module

PM6750 Patient monitor module [77] was made by Shanghai Berry Electronic Tech Co., Ltd. It is a Portable design with flexible installation steps and easy operation making it capable of meeting a variety of requirements. The outer case is shown in Figure 4.5 and is of the size 240mm x 165mm x 50mm. PM6750 monitors multiple vital signs, including SpO2, Pulse Rate, 5-Lead ECG, Heart Rate, Respiration, Body Temperature and Non-Intrusive Blood Pressure (NIBP). The monitor transfers the sensed data to PC or other smart terminals for secondary development through Serial Port, USB or Bluetooth. As shown in Figure 4.6, the PM6750 system sketch has interfaces to connect with ECG leads, Temp probe, SpO2 Sensor and NIBP Cuff to monitors multiple vital signs. Then, the result is sent through Serial Port, USB or

Bluetooth. And the AC adapter supplies power for all functions.

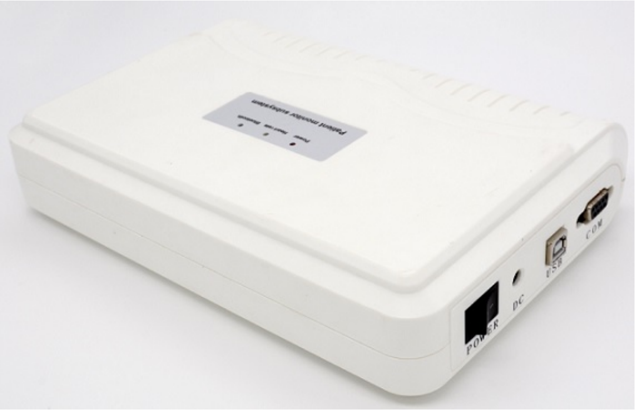


Figure 4.5: The outer case of module PM6750 (240mm x 165mm x 50mm)

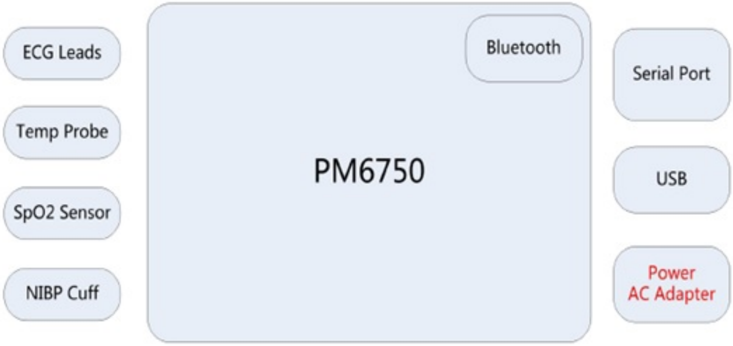


Figure 4.6: PM6750 System Diagrammatic Sketch

1. **Electrocardiogram (ECG) sensor** consists of five-electrode leads which are attached to the patient's body to measure the electrical activity of the heart. ECG electrodes are colour-coded, and each is identified by a specific code that refers to its intended placement. Table 4.1 shows the description of the coding system used. Result is usually displayed in a graph showing voltage versus time of the electrical activity of the heart. To a trained medical practitioner, an ECG reports a large amount of information about the state of the heart and the function of its electrical conduction system. The ECG wave as shown in Figure 4.7. is explained below:

(a) P wave is the first electrical signal on a normal ECG which originates from the atria. It is the sum of the electrical signals from the two atria.

(b) PR segment is a short period where no electrical activity is seen on the ECG. It is represented by a straight horizontal or 'isoelectric' line. It occurs when there is a physiological delay as the atrioventricular (AV) node slows the electrical depolarisation before it proceeds to the ventricles.

(c) QRS complex is when the depolarisation of the ventricles occurs which results in usually the largest part of the ECG signal as a result of the greater muscle mass in the ventricles.

(d) Q wave is the first initial downward or 'negative' deflection.

(e) R wave is the next upward deflection.

(f) S wave is the next deflection downwards.

(g) T wave is an upright deflection of variable amplitude and duration.

(h) ST segment is an electrical signal reflecting repolarisation of the myocardium.

The normal adult ECG reading has a heart rate (HR) of 60-100 beats per minute (bpm), PR interval should be between 120-200 ms (3-5 small squares), QRS duration range up to 120 ms, and QT interval range up to 440 ms [78].

Table 4.1: Code description and location of ECG electrodes

Code	Location	Colour
RA	Right arm (inner wrist)	White
RL	Right leg (inner ankle)	Green
LA	Left arm (inner wrist)	Black
LL	Left leg (inner ankle)	Red
V	Chest	Brown

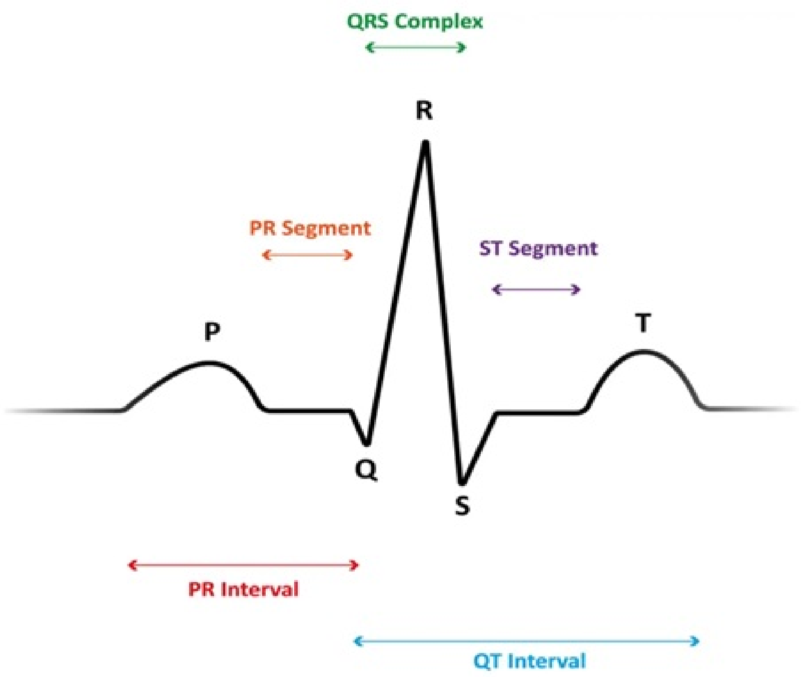


Figure 4.7: The major waves of a single normal ECG pattern

2. **Temperature sensor** is used to measure the temperature of the patient. It can be placed on any part of the body. The normal adult temperature reading ranges between 97 F (36.1 C) and 99 F (37.2 C). An adult with temperature value of 103 F (39.4 C) or higher is considered to be sick or having fever while temperature below 95F (35C) is medically known as hypothermia, which might be an indication of infection.

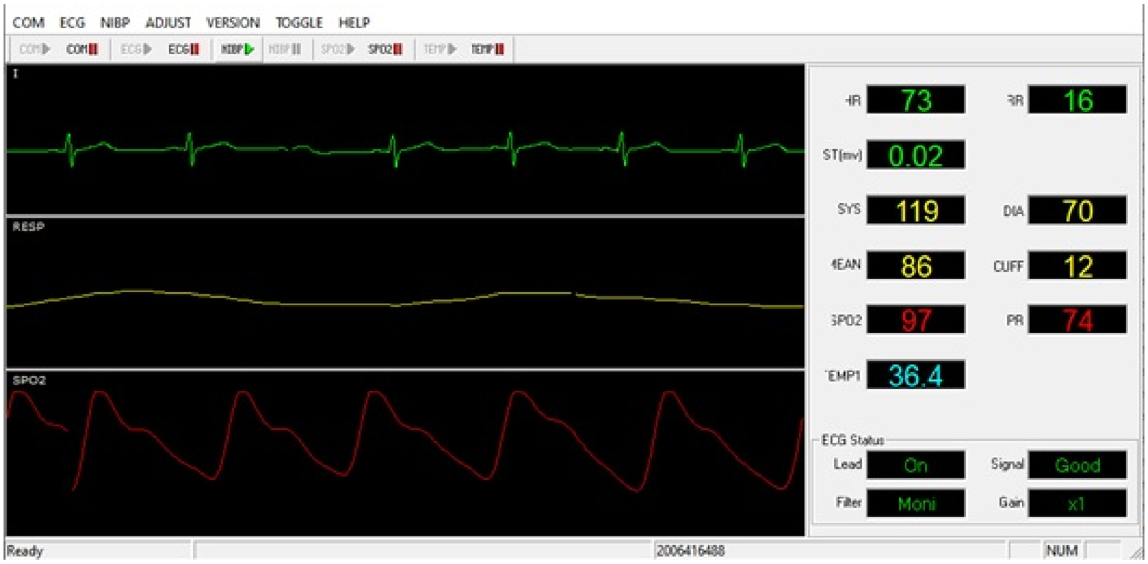
3. **Blood Oxygen Saturation (SpO2) sensor** is used to measure the oxygen level in the patient's blood and the heart rate. It is a small device that clips to your finger. It can be placed on the index figure. Normal pulse oximeter readings usually range from 95 to 100 percent. Values below 90 percent are considered low and may result in various symptoms, such as shortness of breath. It is medically termed Hypoxemia, which is a sign of a problem related to breathing. It usually indicate the need for supplemental oxygen.

4. **Non-invasive blood pressure** is used to measure human blood pressure. It measures systolic, diastolic and mean arterial pressure. It is attached tightly to

the arm for accurate and reliable measurement. A normal blood pressure level is less than 120/80 mmHg. Blood pressure level below 120/80 is considered to be low blood pressure while values above 120/80 is considered to be high blood pressure. Low blood pressure can be dangerous, it can cause dizziness and fainting when the brain fails to receive enough blood. High blood pressure is also risky as it can lead to heart attack, stroke or kidney damage.

The Gateway

We used a Windows-based laptop to serve as the gateway which the multi-sensor board is connected via a USB port. The medical data received from the board is displayed on the Graphical User Interface (GUI) as shown in Figure 4.8, to monitor the patient's biometric data. The gateway sends this real-time data to the IDS for processing before being sent to the monitoring systems. It acts as a relay to the cloud. This process is accomplished by series of process explained in this section. The gateway connects to the switch using Ethernet cable. The GUI shows heart rate (HR) in Beats Per Minute (BPM), Respiration Rate (RR) in BPM, ST in millivolts (mv), Systolic blood pressure (SYS), Diastolic blood pressure (DIA), Mean arterial pressure (MEAN), Blood Oxygen Saturation (SPO2), PR, the inflation of the cuff placement on the arm (CUFF), and temperature (TEMP) in Celsius (C).


COM ECG NIBP ADJUST VERSION TOGGLE HELP
COM▶ COM▮▮ ECG▶ ECG▮▮ NIBP▶ NIBP▮▮ SPO2▶ SPO2▮▮ TEMP▶ TEMP▮▮
I
RESP
SPO2

HR 73 RR 16
ST(mv) 0.02
SYS 119 DIA 70
MEAN 86 CUFF 12
SPO2 97 PR 74
TEMP1 36.4

ECG Status
Lead On Signal Good
Filter Moni Gain x1

Ready 2006416488 NUM

Figure 4.8: PM6750 Communication Protocol after Module is powered displaying patient's biometric reading

Message Queuing Telementry Transport (MQTT) Environment

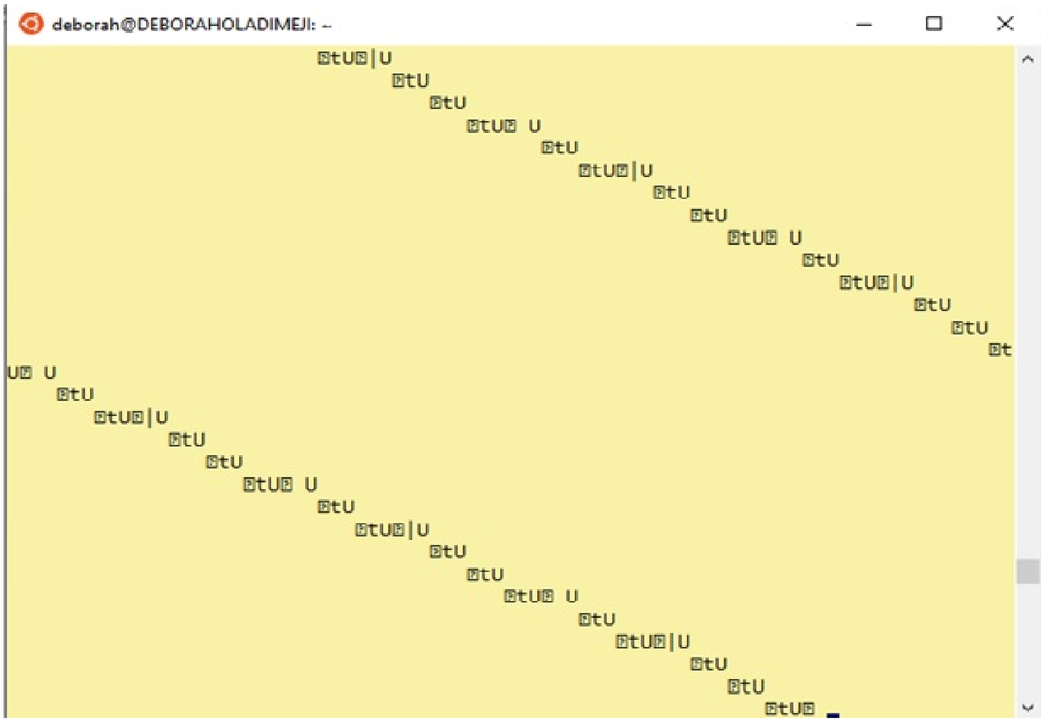
MQTT is a lightweight publish-subscribe protocol that transports messages between devices. It runs over TCP/IP and also supports any network protocol that provides bidirectional connections. It is suitable for a very small, resource-constrained device like IoMT due to its lightweight feature. It uses the topic (subject) of the message to determine which message goes to which client (subscriber). A topic is a hierarchically-structured string that can be used to filter and route messages. MQTT client could either be a publisher or subscriber. Client refers to any device that runs an MQTT library and connects to a MQTT broker over a network. The publisher and subscriber refer to whether the client is currently publishing messages or subscribed to receive messages. The responsibilities of the broker is to receive all messages, filter the messages, determine who is subscribed to each message, and sending the message to these subscribed clients. It authenticates and authorizes the clients.

We set up an MQTT environment on the Windows-based laptop to communicate with the sensors. The code below is used to prepare the MQTT environment after installing Windows Subsystem for Linux (WSL) on Windows 10. The MQTT clients are installed to initiate the communication process.

```
$ sudo apt update
$ sudo apt upgrade
$ which -a cu mosquitto mosquitto_sub mosquitto_pub
$ sudo apt install cu mosquitto mosquitto-clients
```

After which we used the code below to establish a connection with the multi-sensor board. The board works at baud rate of 115200 and is connected to the Windows UART port. The raw data from sensors is displayed on the WSL screen in ASCII format using the "cu" command as shown in Figure 4.9.

```
$ sudo apt update
$ sudo apt upgrade
$ sudo apt install cu
$ sudo chmod 666 /dev/ttyS6
$ cu -s 115200 -l /dev/ttyS6
```



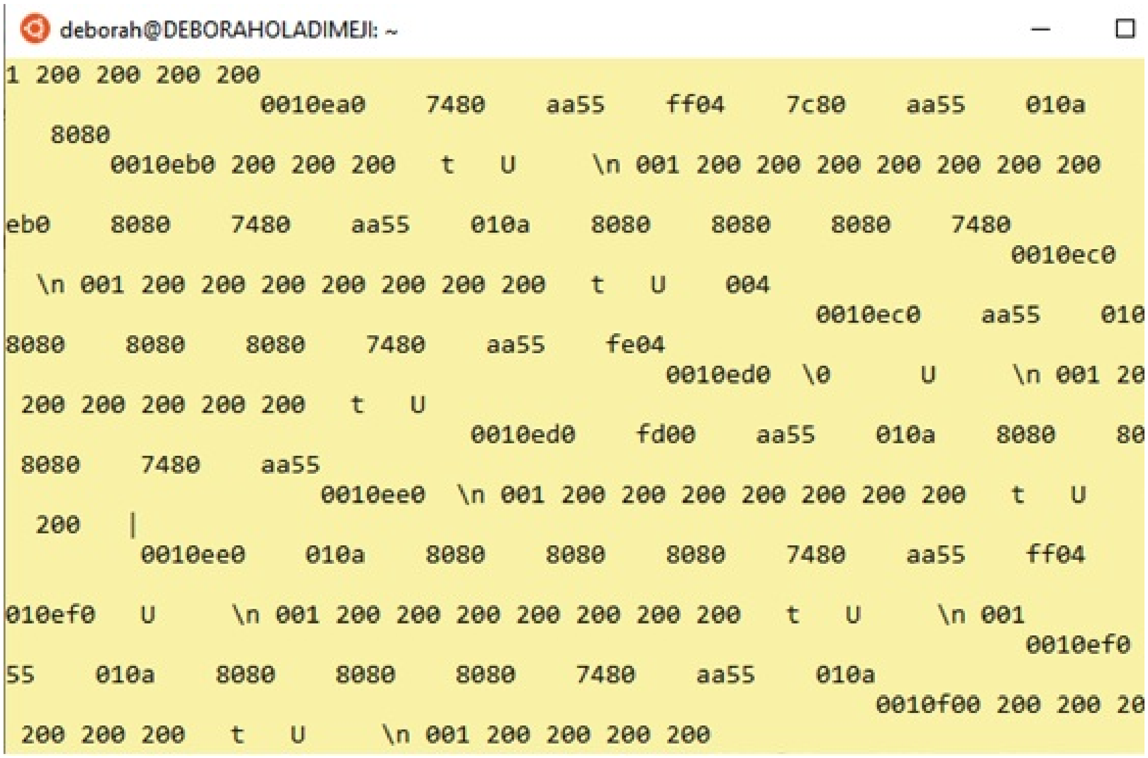
```
                         □tU□|U
                               □tU
                                  □tU
                                     □tU□ U
                                           □tU
                                              □tU□|U
                                                    □tU
                                                       □tU
                                                          □tU□ U
                                                                □tU
                                                                   □tU□|U
                                                                         □tU
                                                                            □tU
                                                                               □t
U□ U
    □tU
       □tU□|U
             □tU
                □tU
                   □tU□ U
                         □tU
                            □tU□|U
                                  □tU
                                     □tU
                                        □tU□ U
                                              □tU
                                                 □tU□|U
                                                       □tU
                                                          □tU
                                                             □tU□
```

Figure 4.9: ASCII output using “cu” command in WSL/Ubuntu

To make sense with the output, the following lines of code is used to convert the ASCII output to hexadecimal with "hexdump" command [79]. This receives the data from the target device in a more readable format shown in Figure 4.10.

```
$ sudo apt install od hexdump
$ which -a od hexdump
$ which -a stdbuf gstdbuf
$ which -a od
$ cu -s 115200 -l /dev/ttyS7 | hexdump -c  x
$ sudo cu -s 115200 -l /dev/ttyS6 | hexdump -c  x
```

The gateway is also responsible for publishing the medical data to the cloud using the following code, for the patient’s biometric data to be viewed at the visualization phase. HiveMQ is the broker used as it is highly scalable, integratable, fault-tolerance and easy to monitor. The topic “deborah/test1” is created to be subscribed to. This code sends data in decimal format as shown in Figure 4.11. The "od" command [80] is used to convert output to decimal format. The first number is

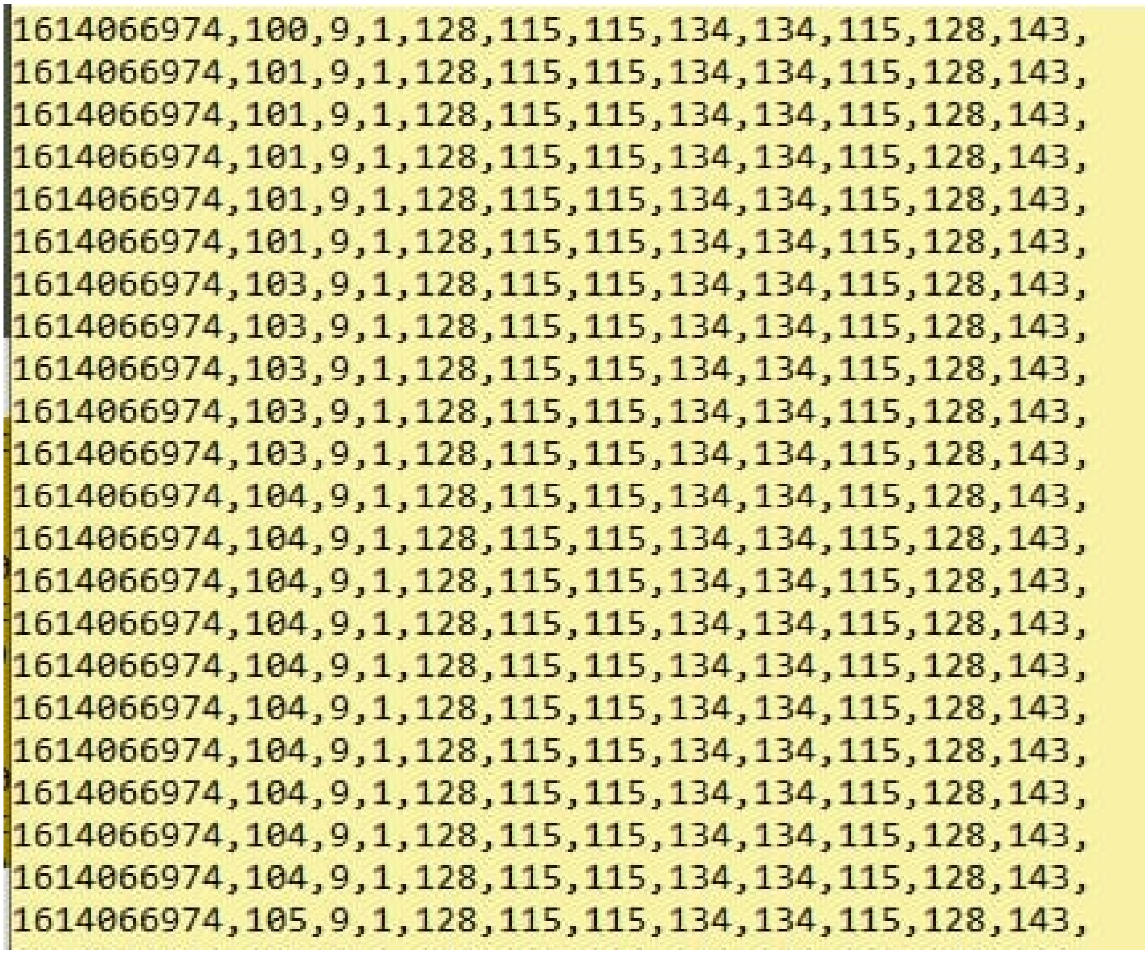


```
1 200 200 200 200
                 0010ea0    7480    aa55    ff04    7c80    aa55    010a
   8080
       0010eb0 200 200 200   t   U     \n 001 200 200 200 200 200 200 200

eb0    8080    7480    aa55    010a    8080    8080    8080    7480
                                                                   0010ec0
  \n 001 200 200 200 200 200 200 200   t   U    004
                                                      0010ec0    aa55    010
8080    8080    8080    7480    aa55    fe04
                                            0010ed0  \0      U     \n 001 20
 200 200 200 200 200   t   U
                               0010ed0    fd00    aa55    010a    8080    80
 8080    7480    aa55
                     0010ee0  \n 001 200 200 200 200 200 200 200   t   U
  200   |
         0010ee0    010a    8080    8080    8080    7480    aa55    ff04

010ef0   U     \n 001 200 200 200 200 200 200 200   t   U     \n 001
                                                                    0010ef0
55    010a    8080    8080    8080    7480    aa55    010a
                                                          0010f00 200 200 20
 200 200 200   t   U     \n 001 200 200 200 200
```

Figure 4.10: Hexadecimal output of PM6750 readings using “hexdump” command in WSL/Ubuntu

the timestamp generated using “awk” command discussed in data collection and processing section.

```
$ sudo chmod 666 /dev/ttyS6
$ sudo cu -s 115200 -l /dev/ttyS6 | od -t u1 |
mosquitto_pub -l -t deborah/test1 -h
broker.hivemq.com -I clientId
```



```
1614066974,100,9,1,128,115,115,134,134,115,128,143,
1614066974,101,9,1,128,115,115,134,134,115,128,143,
1614066974,101,9,1,128,115,115,134,134,115,128,143,
1614066974,101,9,1,128,115,115,134,134,115,128,143,
1614066974,101,9,1,128,115,115,134,134,115,128,143,
1614066974,101,9,1,128,115,115,134,134,115,128,143,
1614066974,103,9,1,128,115,115,134,134,115,128,143,
1614066974,103,9,1,128,115,115,134,134,115,128,143,
1614066974,103,9,1,128,115,115,134,134,115,128,143,
1614066974,103,9,1,128,115,115,134,134,115,128,143,
1614066974,103,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,104,9,1,128,115,115,134,134,115,128,143,
1614066974,105,9,1,128,115,115,134,134,115,128,143,
```

Figure 4.11: Decimal output of PM6750 readings using “od” command in WSL/Ubuntu

Network phase

This phase consists of the IDS computer, the router and the attacker. A router is connected to a switch to assign IP addresses for all computers dynamically. The gateway connects to the internet via a Wi-Fi connection to this router. The IDS computer contains the ML models discussed later in this section. It also runs Argus network flow monitoring software. The default configuration of Argus is used with Argus access port to be 561. This extracts the network flow metrics from a network protocol analyser, Wireshark. The concurrent biometric data from the multi-sensor board is also received, and both are processed and analysed with various ML models. This computer checks consistency and makes real-time decision for both network traffic and patient’s biometric data to determine if there are any anomalies. The attacker is an MQTT client used to launch attacks to the system. We imitate different attack scenario in IoMT systems which are dangerous to the network. These attacks are data modification and insertion of patients' biometric data which can cause a wrong diagnosis or treatment. We also launch DoS attacks which include ARP request, ICMP Echo, TCP SYN, UDP flood using the Hyeane software.

Visualization phase

We emulated different monitoring systems to be an Ubuntu-based computer connected via MQTT. They subscribed to the topic and view data in real-time. Patient's biometric data is collected from the gateway to the monitoring system for storing and also analysis by medical practitioner for informed medical decision to be made. With this a medical practioner can be anywhere to monitor his patient's health. For MQTT connection to be established between a client and the broker, clients sends a CONNECT request to the broker, and the broker responds with an acknowledged message CONNACK and a status code. The systems subscribed to the topic created by the gateway (deborah/test1) to get access to the medical data. This is depicted in Figure 4.12 [81]. Once the connection is established, the broker keeps it open until the client sends a disconnect command or the connection breaks. The following lines of code establish connection with the monitoring systems:

```
$ mosquitto
$ mosquitto_sub -t deborah/test1 -h broker.hivemq.com
-I clientId
```

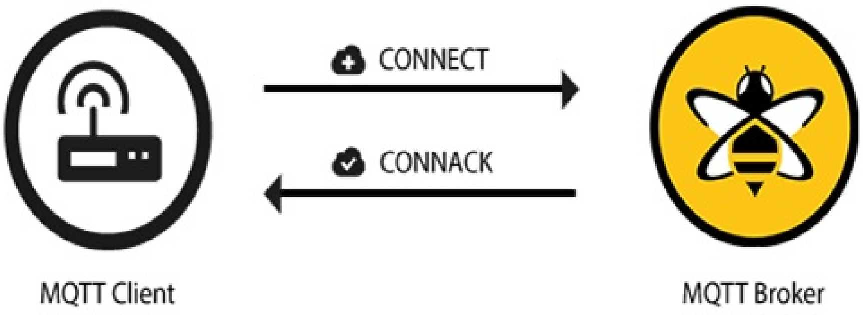


Figure 4.12: MQTT connection establishment between a Client and a Broker

4.4.1 Data Generation and Collection

Data collection is the first step of the intrusion detection system, where network data and biometric data are collected and processed for training and testing the ML methods. Data collection and processing phases characterizes network traffic and biometric data using wide range of features such as source byte, Destination byte, total packet count, heart rate, pulse rate etc. Table 4.2 Shows all the data features used for training and testing. Twenty thousand data set were generated for both normal and attack traffic, labelled as 1 for normal (non-attack) traffic. The attack traffic are labelled as 2 for MitM traffic, 3 for ARP request traffic, 4 for ICMP echo traffic, 5 for TCP SYN traffic, and 6 for UDP flood traffic.

Normal data when the system is free from attack is collected on the IDS by collecting both the raw data from the multi-sensor board and combining with the corresponding network traffic data using the timestamp generated with the biometric data. As shown in Figure 4.11., the data generated from the multi-sensor board are composed of the biometric reading and other board parameters. Therefore, only biometric data are extracted using the following command below. A shell script "doit2.sh" is also used in reading data from the multi-sensor board.

```
$ mosquitto_sub –t deborah/test1 –h broker.hivemq.com –I
clientId  | awk '{for(i=2;i<=NF;i++){printf "%s\n",$i}}'
$ mosquitto_sub –t deborah/test1 –h broker.hivemq.com –I
clientId | awk '{for(i=2;i<=NF;i++){printf "%s\n",$i}}'|
sh ~/doit2.sh | egrep '^.,[2345],'
```

This data is automatically saved in a CSV file for further analysis using the following command:

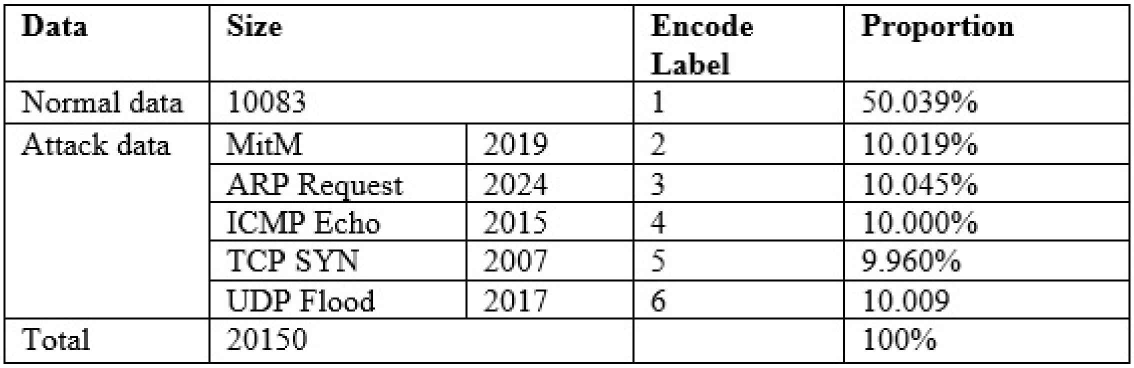
```
$ mosquitto_sub –t deborah/test1 –h broker.hivemq.com –I
clientId | awk '{for(i=2;i<=NF;i++){printf "%d %s\n",
systime(),$i; fflush()}}'| sh ~/doit2a.sh | egrep '
^.*,.,[2345],'| tee ~/new.csv
```

To collect network data, Wireshark and Argus tools are used. While Wireshark is running, Argus is used to extract useful network data from pcap files, generating a csv file. Both Argus csv output and biometric csv data are combined together forming a data sample for the ML algorithms. The generated dataset details are shown in Figure 4.13.

Table 4.2: Machine Learning Features

Metric	**Description**	**Type**
Dir	Direction of transaction	Network flow metric
SrcAddr	Source IP address	Network flow metric
DstAddr	Destination IP address	Network flow metric
Proto	Transaction protocol	Network flow metric
Sport	Source port number	Network flow metric
Dport	Destination port number	Network flow metric
SrcBytes	Source to destination transaction bytes	Network flow metric
DstBytes	Destination to source transaction bytes	Network flow metric
SrcLoad	Source bits per second	Network flow metric
DstLoad	Destination bits per second	Network flow metric
SrcGap	Source bytes missing in the data stream	Network flow metric
DstGap	Destination bytes missing in the data stream	Network flow metric
SIntPkt	Source interpacket arrival time	Network flow metric
DIntPkt	Destination interpacket arrival time	Network flow metric
SIntPktAct	Source active interpacket arrival time	Network flow metric
DIntPktAct	Destination active interpacket arrival time	Network flow metric
SrcJitter	Source jitter	Network flow metric
DstJitter	Destination jitter	Network flow metric
sMaxPktSz	Maximum packet size for traffic transmitted by the source	Network flow metric

dMaxPktSz	Maximum packet size for traffic transmitted by the destination	Network flow metric
sMinPktSz	Minimum packet size for traffic transmitted by the source	Network flow metric
dMinPktSz	Minimum packet size for traffic transmitted by the destination	Network flow metric
Dur	Record total duration	Network flow metric
Trans	Transport information	Network flow metric
TotPkts	Total transaction packet count	Network flow metric
TotBytes	Total transaction bytes	Network flow metric
Load	Bits per second	Network flow metric
Loss	Packets retransmitted or dropped	Network flow metric
pLoss	Percent packets retransmitted or dropped	Network flow metric
Rate	Packets per second	Network flow metric
SrcMac	Source MAC address	Network flow metric
DstMac	Destination MAC address	Network flow metric
ECG Param (Heart Rate)	Heart rate	Biometric
ECG Param (Resp Rate)	Respiration rate	Biometric
NIBP Param (SYS)	Systolic blood pressure	Biometric
NIBP Param (DIA)	Diastolic blood pressure	Biometric
SPO2 Param(SPO2)	Blood oxygen saturation	Biometric
SPO2 Param(Pulse Rate)	Pulse rate	Biometric
TEMP Param	Temperature	Biometric



Data	Size		Encode Label	Proportion
Normal data	10083		1	50.039%
Attack data	MitM	2019	2	10.019%
	ARP Request	2024	3	10.045%
	ICMP Echo	2015	4	10.000%
	TCP SYN	2007	5	9.960%
	UDP Flood	2017	6	10.009
Total	20150			100%

Figure 4.13: Generated Dataset of Normal and Attack traffic

4.4.2 Data Processing

Data preprocessing is an integral step in ML that helps improves the quality of data to enhance the extraction of useful information. The meaningful data derived from it directly affects the ability of our model to learn, therefore, it is extremely important that we preprocess our data before feeding it into our model. The following steps describe the steps followed to preprocess the network flow metrics and biometric data:

1. **Handling null values:** In the dataset, there are few null values. We used a Jupyter notebook to check if there are null values in our dataset. The columns are transformed by deleting the null values and converting string to integer.

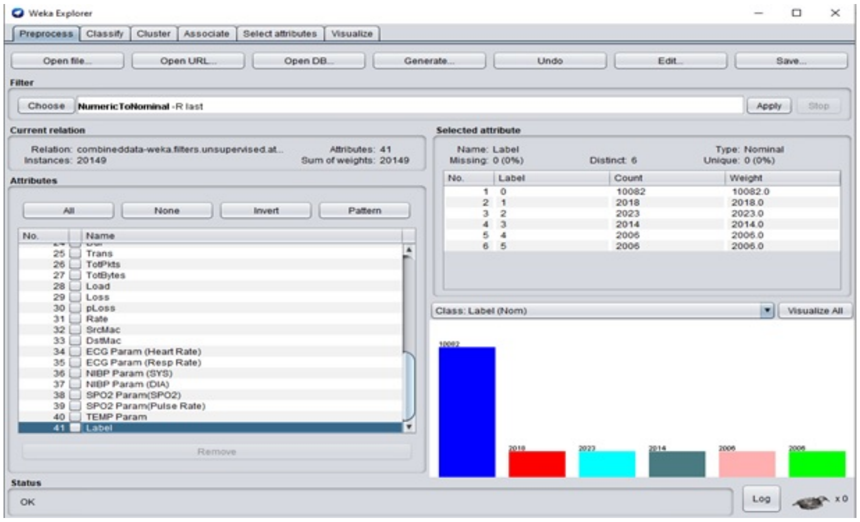
2. **Handling zeros:** There are a lot of zeros generated in the dataset especially in the attack traffic. The zeros values are left untouched as they are valid values produced during attack when the patient's biometric data are not able to be transported to the monitoring systems from the gateway.

3. **Cross-validation folds:** This includes splitting the original dataset into k equal parts (folds). It takes out one fold aside, and performs training over the rest k-1 folds and measures the performance. Then, repeats the process k times by taking different fold each time. Cross-validation is used to overcome the problem of overfitting and makes the predictions more general [82]. We have assigned k to be equals to 10. Our dataset is divided into 10 equal folds. One

fold is set aside in each iteration. Each fold is then used once for testing and nine times for training.

4.4.3 Machine Learning Models for Classification

For monitoring a patient, the ML-based methods will analyse the situation according to the trained dataset. Our dataset consists of 10,000 normal samples and 10,000 attack, 2,000 for each type of attack launched, making a total of 20000 samples. We have used cross validation with k set to 10. We implemented different ML models before selecting the top six that gives the most promising result. The six supervised ML algorithms for training and testing to test our proposed intrusion detection system are RF, KNN, SVM, ANN, J48 and DT. We have analysed all types of dataset (network-data, biometric-data, and combined-data) them with the help of the Waikato Environment for Knowledge Analysis (WEKA) platform. WEKA is an open-source data-mining tool based on the Java programming language. It was designed and developed at the University of Waikato, New Zealand. WEKA is mainly used for data-mining tasks and for modelling machine-learning algorithms. WEKA supports several data-mining tasks such as data pre-processing, data clustering, feature selection, and regression [83]. Figure 4.14. shows entire dataset analysed in Weka explorer. To give an overview of the concept, detail explanation of these methods is provided in this section.



Filter: NumericToNominal -R last

Relation: combineddata-weka.filters.unsupervised.at... Attributes: 41
Instances: 20149 Sum of weights: 20149

No.		Name
25	□	Trans
26	□	TotPkts
27	□	TotBytes
28	□	Load
29	□	Loss
30	□	pLoss
31	□	Rate
32	□	SrcMac
33	□	DstMac
34	□	ECG Param (Heart Rate)
35	□	ECG Param (Resp Rate)
36	□	NIBP Param (SYS)
37	□	NIBP Param (DIA)
38	□	SPO2 Param(SPO2)
39	□	SPO2 Param(Pulse Rate)
40	□	TEMP Param
41	□	Label

Name: Label Type: Nominal
Missing: 0 (0%) Distinct: 6 Unique: 0 (0%)

No.	Label	Count	Weight
1	0	10082	10082.0
2	1	2018	2018.0
3	2	2023	2023.0
4	3	2014	2014.0
5	4	2006	2006.0
6	5	2006	2006.0

Class: Label (Nom)

OK

Figure 4.14: Weka explorer showing the combined dataset for further analysis

Random Forest (RF)

RF consists of a large number of individual decision trees that operate as an ensemble. Each individual tree in the random forest spits out a class prediction and the class with the most votes becomes the model's prediction [12]. Random Forest consists of multiple decision trees with each taking a different feature subset to train and test. The prediction of the random forest model can be executed by the majority or weighted voting by the individual trees. The decision trees may have different effect on different features based on the decision trees. For instance, different prediction might be generated by the decision trees in the random forest for the same data. A simple way of addressing this issue is by utilizing a voting mechanism [84]. Some of advantages of Random Forest include but not limited to its resistance to overfitting and a low number of model parameters required. Although, the number of trees increases in a random forest, the bias is not affected by the decrease in the variance of the model. The random forest has some limitations, such as its dependence on a random generator and low interpretability [85].

K-Nearest Neighbor (KNN)

KNN is a ML model that classifies data points based on the points that are most similar to it [13]. It supports both classification and regression. It initially by stores the whole training dataset and queries it to locate the k most similar training patterns when making a prediction. KNN take the most common class (mode) of the k most similar instances in the training dataset to make predictions on classification problems. K parameter controls the size of the neighbourhood. The value of k determines how predictions are made. For example, if k is 1, then predictions are made using single most similar training instance to a given new pattern for which a prediction is requested. In our analysis, we have set Weka to automatically find a good value for k by setting the crossValidate parameter to True using the cross validation inside the algorithm. Also, the default nearestNeighbourSearchAlgorithm parameter, LinearNNSearch is used. This dictates the manner of storage and searching the training data [64].

Support Vector Machine (SVM)

SVM uses a hyperplane in an N-dimensional space to classify the data points [15]. N is the number of features which is 42 in our dataset. The classifier is based on finding a hyperplane that differentiates two classes in a way that the distance between the hyperplane and the closest point of a class is maximized. Various types of classification can be carried out by controlling the application of SVM kernels such as linear, polynomial, Gaussian radial basis function, and hyperbolic tangent [84]. SVM is mainly used for carrying out binary classification, but it can also be applied for multi-class classification by finding the optimal hyperplane between each pair of classes. The SVM used for our dataset is linear SVM, which is a parametric method.

Artificial Neural Networks (ANN)

ANN is a model that is vaguely inspired by the biological neural networks [16]. A neural network is an information processing technique which consists of a collection of processing units called neurons that are highly interconnected based on a given topology. ANN is capable of learning by example and generalize from limited, incomplete, and noisy data. It works like the way human brain processes information. ANN includes a large number of connected processing units that work together to process information, and also generate meaningful results from it. An ANN first goes through a training phase where it learns to recognize patterns in data. The type of ANN used is MultilayerPerceptron with batchSize of 100, normalizeAttributes set to be "true", and validationThreshold set to 20. During this supervised phase, the network compares its actual output produced with the desired output. The difference between both outputs is adjusted using back propagation. This implies that the network works backward, adjusting the weight of its connections from the output unit to the input units until the difference between the actual and desired outcome produces the lowest possible error [86]. In addition to its use in classification in a large amount of data, it can be applied for regression of continuous target attributes.

J48

J48 is a decision tree classifier that uses a predictive machine-learning model which calculates the resultant value of a new sample based on various attribute values of the available data [17]. It is an advanced decision tree algorithm sometimes referred to C4.5 algorithm. As a decision tree classifier, J48 uses a predictive machine-learning model that calculates the resultant value of a new sample based on various attribute values of the available data. The internal nodes of a decision tree indicate it different attributes. The values of these attribute can have in the observed samples is dictated by the branches between the nodes, while the terminal nodes determines the final classification of the dependent variable. Other J48 features include decision trees pruning, deriving rules, accounting for missing values, continuous attribute value ranges, etc [17]. J48 gives the most promising result in our analysis achieving an accuracy of 98.66% for combined dataset.

Decision Tree

Decision Tree is a model used for specifying which actions to perform depending on given conditions. It is mostly used by researchers to detect DoS attacks. It breaks down a set into smaller subsets to construct a tree comprising decision nodes and leaf nodes. Decision nodes branch out to possible decision paths. Leaf nodes represent a final classification or decision. Decision Tree performs the detection of the types of attacks by calculating the information gain at every split point [84]. It calculates the information gain by measuring the difference of information purity before and after splitting. The normalized information gain is calculated for each node while building the tree. The feature containing the highest value of information gain is chosen for making decisions. The decision tree recursively continue in this manner until all the samples of the dataset are classified. One of the significant advantages of the decision tree is that it calculates the biased information gain values for the categorical features. Although, rules extracting rules from wider and deeper decision trees are complex but it provides excellent accuracy [85].

Chapter 5

Experimental Results and Discussion

5.1 Results and Evaluation

In this section, we present two sets of results to validate that the network parameters and biometric data have an effect for detecting the presence of MitM and DoS attacks in the network. First, we generated dynamic graphs using gnuplot [87], a command-line program that can generate two- and three- dimensional plots. The dynamic graphs gives real-time data view of patient's biometric reading on the monitoring systems. Secondly, we present the results of the metrics used for all ML classifiers.

Figure 5.1 shows normal heart rate reading without attack while Figure 5.2 and Figure 5.3 both show heart rate during MitM attack explained above.

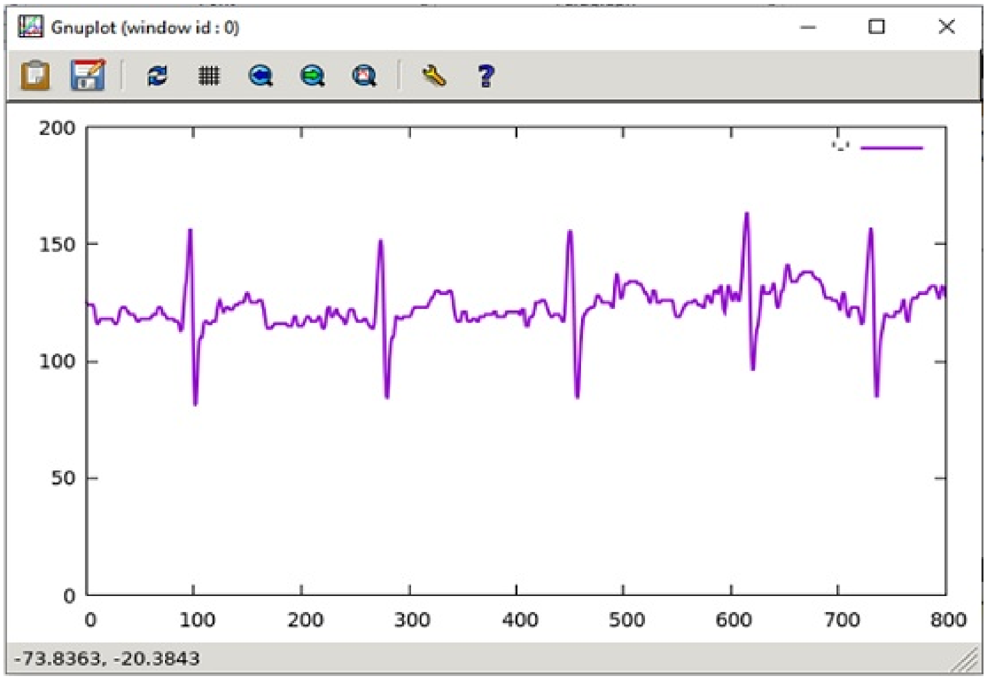


Figure 5.1: Result of normal data shown on monitoring systems

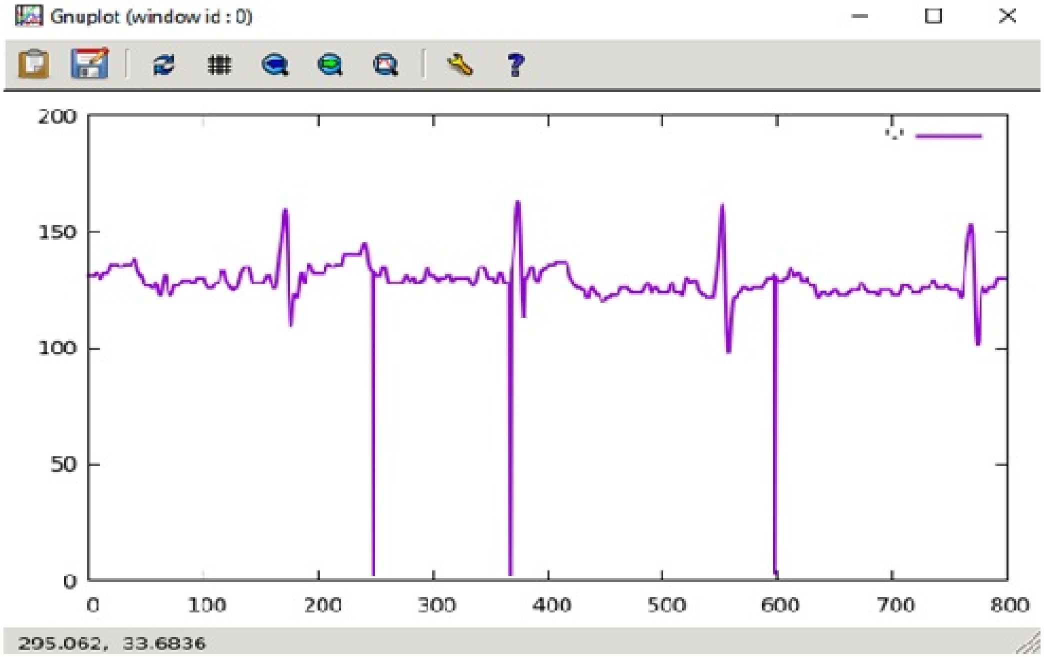


Figure 5.2: Result of data modification/insertion attack shown on monitoring systems

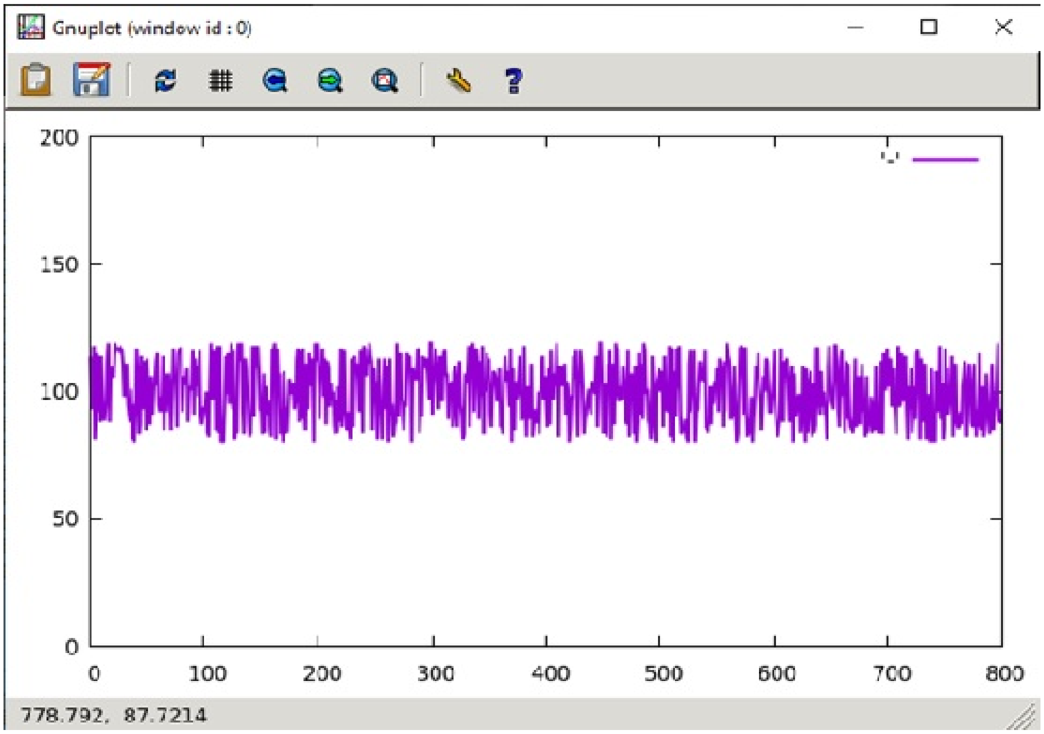


Figure 5.3: Result of data modification/insertion attack shown on monitoring systems

The metrics used for the evaluation of the ML algorithms for intrusion detection are explained in this section. To check the validity of using ML to differentiate between normal and attack biometric data, we compared the six ML methods used based on their performances using Accuracy, Execution time, Area under the ROC (AUC) score, Precision, Recall, F1 score, True Positive, and False Positive.

Accuracy

Accuracy is the number of correctly predicted data points out of all the data points. It is the fraction of predictions our model got right. It is defined as the number of true positives (TP) and true negatives (TN) divided by the number of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). The percentage of correctly classification for this IDS is expected to be high for "combineddata" in all the ML methods used. Figure 5.4. shows the accuracy results for all six models built with only biometrics features, only network features, and combined features. As can be seen, all models perform better with combined features compared to only biometrics features and only network features. This indicates that using combined features provides better results than using only one of the two types of features. J48 performs significantly better than the rest of the models. Accuracy does not give the full picture of how FP and FN affect the result, therefore we have considered other metrics for evaluation. Accuracy can be represented as:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{5.1}$$

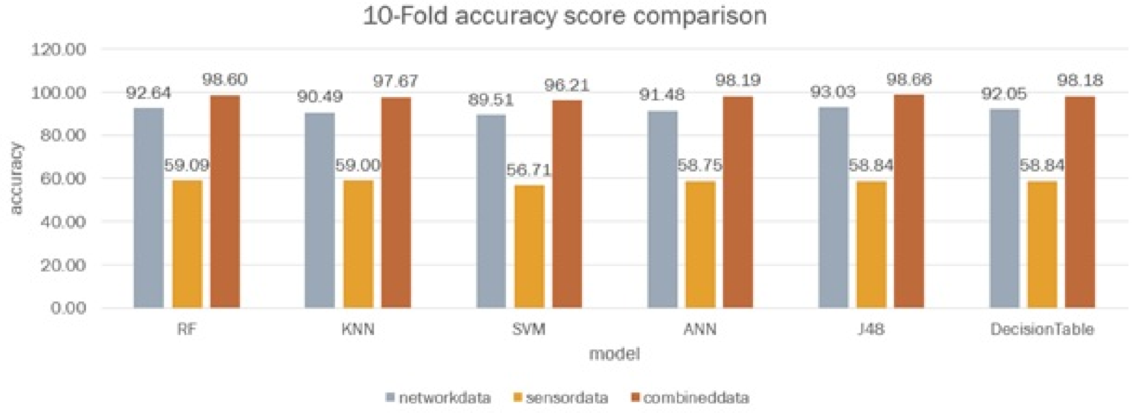


Figure 5.4: 10-Fold accuracy score comparison for all models

Execution Time

This is the execution time for all the models to make prediction between normal and attack data. Since we used cross-validation, WEKA only provides the time taken to build the model which is the training time. As shown in Figure 5.5, the execution times for RF, J48, and DT are below 12 seconds for different categories of features. KNN is seen to have the least execution times while SVM and ANN have considerable high execution times across different types of features. Considering real-time requirement of health system which makes every second count, KNN proves to deliver the least time for all the features.

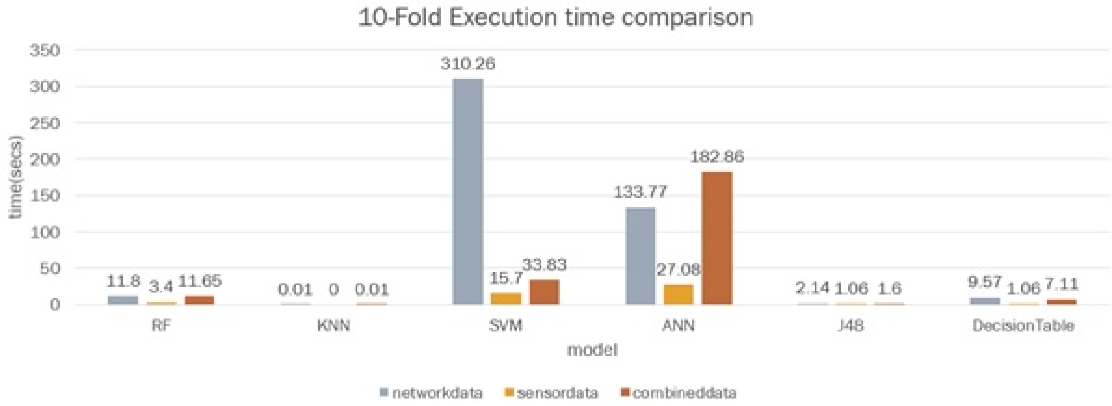


Figure 5.5: 10-Fold execution time comparison for all models

AUC Score

AUC measures the entire two-dimensional area underneath the entire Receiver Operating Characteristic (ROC) curve. ROC curve is a graph showing the performance of a classification model at all classification thresholds. AUC is an efficient sorting-based algorithm to compute the points in an ROC curve. AUC gives an aggregate measure of performance across all possible classification thresholds. AUC ranges in value from 0 to 1. A model whose predictions are 100% wrong has an AUC of 0.0 while one whose predictions are 100% correct has an AUC of 1.0. Our model's AUC score ranges from 0.593 – 0.796 for only network feature, 0.920 – 0.979 for only biometric feature, and 0.983 – 0.999 for combined data. As shown in Figure 5.6, the AUC scores confirm the advantage of using combined features compared to only one feature.

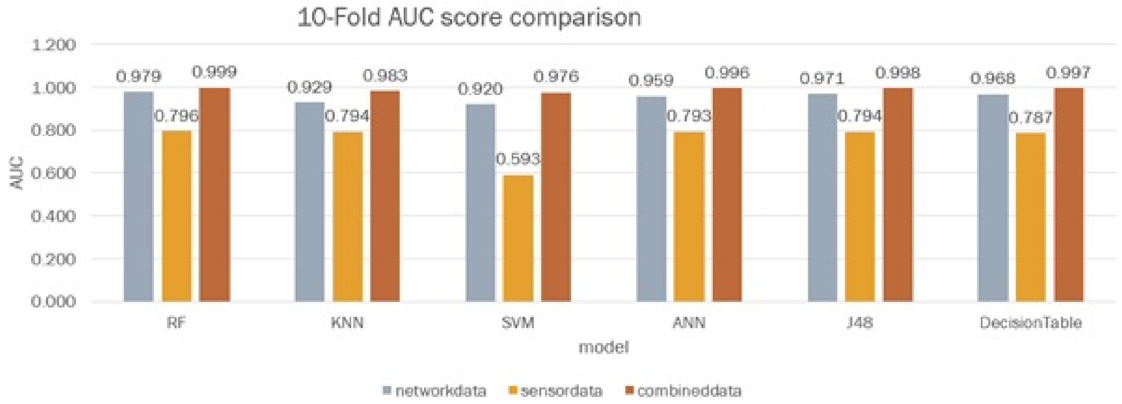


Figure 5.6: 10-Fold AUC score comparison for all models

Precision

Precision is the ratio of correctly predicted positive observations to the total predicted positive observations. High precision relates to the low false positive rate. As shown in Figure 5.7., we have got 0.905, 0.591 and 0.987 as the highest precision score for only network data, only biometric data and combined data respectively. Precision can be represented as below:

$$Precision = \frac{TP}{TP + FP} \tag{5.2}$$

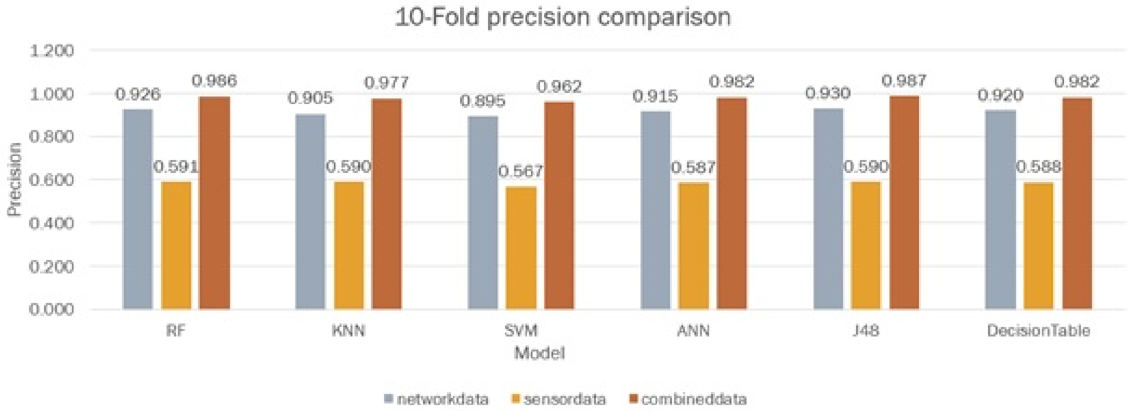


Figure 5.7: 10-Fold Precision comparison for all models

Recall

Recall is defined as the fraction of samples which were predicted to belong to a class with respect to all of the samples that truly belong in the class. Recall is a very useful metric which measures the correctly classified instances against all the predicted system call traces of that specific class. Figure 5.8 shows the 10-fold recall scores for all ML models. As seen, we have got recall scores of 0.930, 0.591 and 0.987 for only network data, only biometric data and combined data respectively. This is good for this model as it is above 0.5. Recall can be formulated as:

$$Recall = \frac{TP}{TP + FN} \tag{5.3}$$

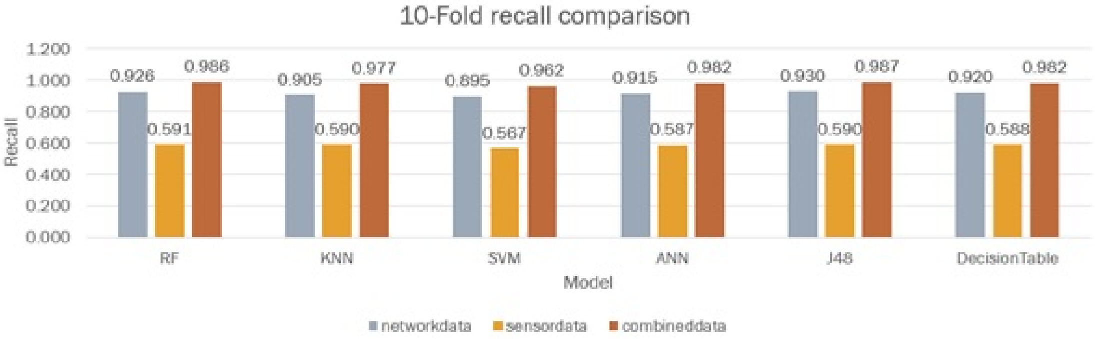


Figure 5.8: 10-Fold Recall comparison for all models

F1 Score

To fully evaluate the effectiveness of our model, we also calculate F1 score. F1 score is the overall measure of the accuracy of a model accuracy that combines precision and recall. A good F1 score means there are low false positives and low false negatives. Our model is able to correctly identify threats and no disturbance with false alarms. A value of 1 means a perfect F1 score while 0 means the model is a total failure. As shown in Figure 5.9, we have achieved a F1 score of 0.925, 0.750, and 0.987 as the highest for only network feature, only biometric feature, and both combined feature. This indicates that combined feature gives a better result for the model. F1 score can be represented as:

$$F1Score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{5.4}$$

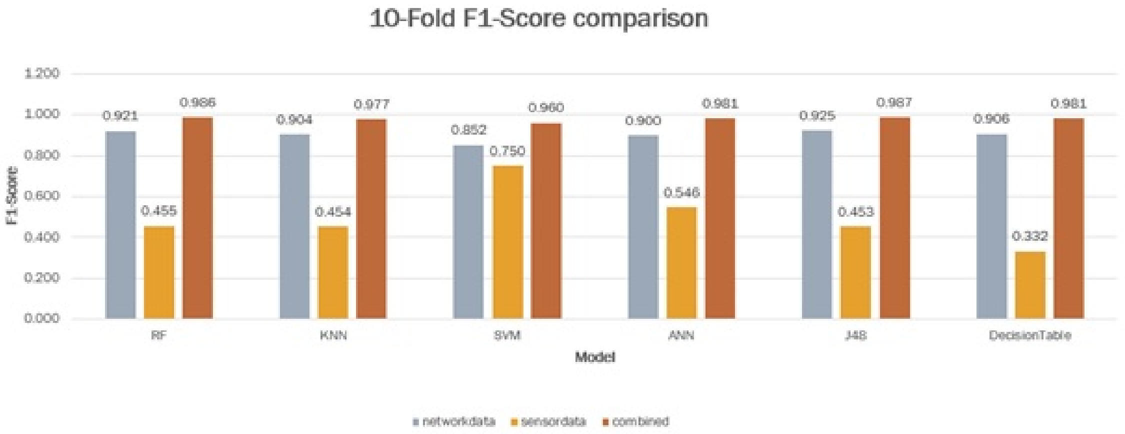


Figure 5.9: 10-Fold F1-Score comparison for all models

True Positive (TP)

TP is when a model correctly predicts the positive class. As shown in Figure 5.10, a higher TP is achieved for combined features compared to only one feature. This shows that the positive class is correctly classified, and also an indicator that using the combination of biometric and network data gives a better result than only either of the two.

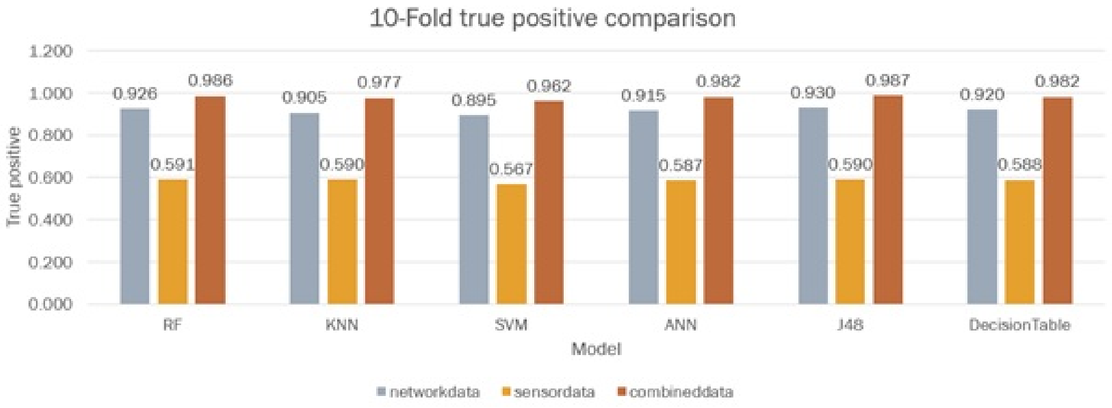


Figure 5.10: 10-Fold True positive comparison for all models

False Positive

False Positive (FP) is an outcome where the model incorrectly predicts the positive class e.g. normal records incorrectly classified as attack records. A lower FP is desirable since we want to correctly classify the positive class. As seen in Figure 5.11 we got 0.054, 0.410 and 0.009 as the least FP value for only network data, only biometric data and combined data respectively. The FP rate decreases in combined features as as result of the increase in the number of features.

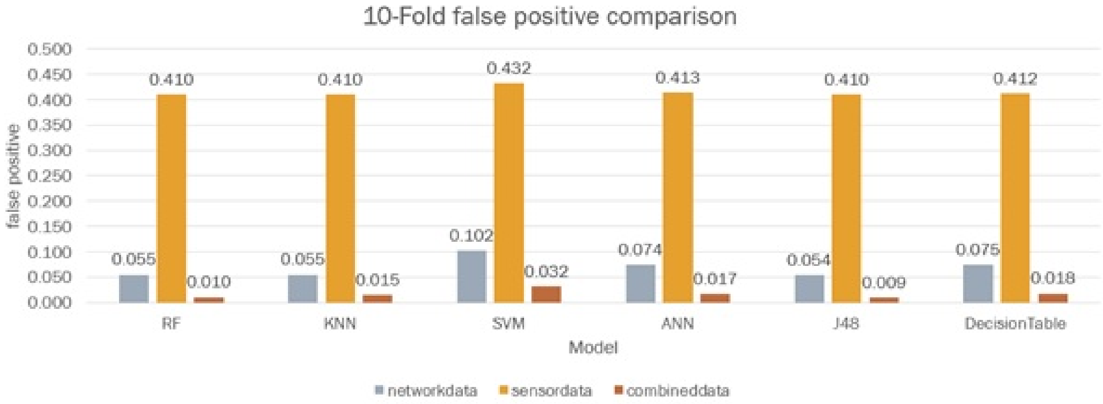


Figure 5.11: 10-Fold False Positive comparison for all models

5.2 Comparison Analysis Anar et al. [74]

This section describes the comparative analysis between the proposed scheme and existing scheme. Not much work has been done in this area, the only related work done by Anar et al. [74] is thus considered for comparison. Table 5.1 shows the summary of the comparison in experimental setup while Table 5.2 shows the comparison in results. As seen in Table 5.1, we have provided the cloud option for the IDS through MQTT protocol. This gives the healthcare provider the ability to remotely monitor the patient's health and also enable the system administrator remote access to continually monitor the network. While the existing technique has generated 16000 samples in which 14000 is the normal samples and 2000 is the attack samples with the use of 34 features for their ML models, our generated dataset consists of 10000 normal samples, 2000 attack samples for each attack launched, making a total of 20000 with the use of 42 features for our ML models. This can be attributed to the increase in the efficiency of our IDS as ML models gives more promising result with larger dataset with more feature.

Table 5.1: Comparison analysis of experimental setup

Parameters	Existing technique (Anar et al. [74])	Proposed technique
Communication Protocol	Wi-fi using TCP/IP protocol	MQTT protocol to interface IoMT devices
Attack Vector	MitM (Spoofing and Data modification)	MitM – Data insertion/Data modification DoS – ARP Request, ICMP Echo, TCP SYN, UDP Flood
Output Labels	2 (Normal and attack vector)	6 (Normal and attack data for each attack)
ML Models	RF, KNN, SVM, ANN	RF, KNN, SVM, ANN, J48, DT
Number of Features	34	42
Total Dataset	16000	20000

(Anar et al. [74]) argued that ANN is the best model for the healthcare system. However, after thorough consideration of the ML models, we concluded that KNN is the best model for IDS in healthcare system. This is majorly due to its low execution time, as time is a very crucial determinant of efficiency of healthcare system. We chose to compare the result of the ML models on combined features only since all methods proves to achieve better results with combined features as against using only either of the two. As seen in Table 5.2, ANN gives an accuracy of 97.67 and AUC score of 0.983 which are considered to be a very good measure of validation of the proposed IDS. In addtion to these differences, the major significant differences between the two works is that, our model is able to scale easily, an advantage derived from the use of MQTT, and also gives the lowest execution time of 0.01 which is 27210 times lower.

Table 5.2: Comparison analysis of result

Metrics	(Anar et al. [74])	Proposed IDS
Accuracy	93.42	97.67
AUC Score	0.929	0.983
Optimal Model	ANN	KNN
Execution Time	272.10	0.01

5.3 Discussion

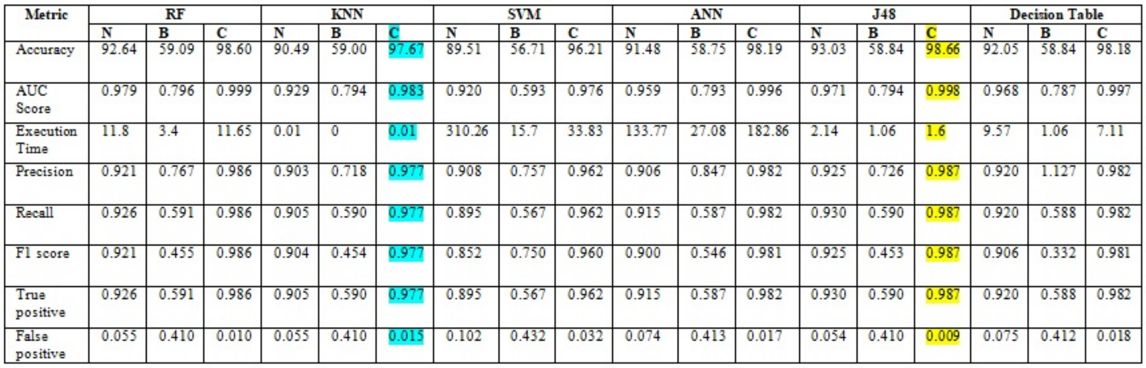
The purpose of the proposed IDS is to be able to detect anomalies in healthcare monitoring system. 20000 dataset has been generated with 42 unique features, 35 being network flow metrics and 7 being biometric data. The size of our dataset performs effectively with the ML algorithms used, since majority of the algorithms are comfortable with small dataset. However, with large dataset, better prediction will be made by the model. Data preprocessing was performed on all the features by handling the null and zero values efficiently. The ML models are trained and tested with only network data, only biometric data, and both data to determine the best features that give more promising result. The merged data of both biometric and network feature was split into training and testing. The training data was used to train the machine learning models. The samples from the testing dataset were used to provide a generalized and an unbiased evaluation of the trained learning model. 10-fold cross-validation was used to evaluate the learning models.

We evaluated the effectiveness of the ML techniques by using some vital metrics including accuracy, AUC score, execution time, precision, recall, F1 score, true positive, and false positive. In addition to this gnuplot is used to display graphs of biometric data reading during normal traffic and attack traffic. The execution time was given utmost importance because of the time-sensitive nature of healthcare system effectively. The true positive indicates how well the model can detect an attack. The false positive rate indicates the efficiency of classifiers to evaluate the miss-classification of the samples that are considered to be attack vector. Table 5.3 shows the total transaction packet count, flow per second, and average packets per second of each traffic. Figure 5.12 summarizes the performance of machine learning classifiers for the healthcare intrusion detection system across all data where N is the network feature, B is the biometric feature, and C is the combined feature. As shown in Figure 5.12, six models perform differently on different dataset. All the classifiers perform better with the combined feature as against when only one feature is used. Although J48 gives the highest performance for combined data compared to other methods with an accuracy of 98.66, AUC score of 0.998, precision to be 0.987, recall of 0.987, F1 score of 0.987, true positive to be 0.987, and false positive to be 0.009. However, its execution time is 1.6 which is about 160 times the execution time of KNN. As this is significantly high considering the real-time requirement of the system, KNN which gives the lowest execution time of 0.01 is considered to be the best model for the healthcare monitoring system.

We could arguably conclude that using both network flow metrics and patient's biometric data enhanced the ML methods for securing health monitoring systems. We proved that the combination of the network parameters and biometric data used in our proposition have a great effect on the detection and identification of all the MitM and DoS attacks launched in the IoMT system. In addition to this, these results show that not all ML methods are suitable for health monitoring systems, especially in terms of execution time. KNN requires the lowest execution time compared to the other ML methods.

Table 5.3: Comparison analysis of traffic size

Features/ Traffic	Normal	MitM	ARP Request	ICMP Echo	TCP SYN	UDP Flood
Number of Packets (bytes)	58.18	70.69	2.82	2.17	2.16	0.00
Size of load(bits/s)	9919429	9908277	64129711	29990379	52514767	24380952
Average Number of Packets (bytes)	3662.83	3901.98	133630.50	89240.13	121589.70	1117366.90



Metric	RF			KNN			SVM			ANN			J48			Decision Table		
	N	B	C	N	B	C	N	B	C	N	B	C	N	B	C	N	B	C
Accuracy	92.64	59.09	98.60	90.49	59.00	97.67	89.51	56.71	96.21	91.48	58.75	98.19	93.03	58.84	98.66	92.05	58.84	98.18
AUC Score	0.979	0.796	0.999	0.929	0.794	0.983	0.920	0.593	0.976	0.959	0.793	0.996	0.971	0.794	0.998	0.968	0.787	0.997
Execution Time	11.8	3.4	11.65	0.01	0	0.01	310.26	15.7	33.83	133.77	27.08	182.86	2.14	1.06	1.6	9.57	1.06	7.11
Precision	0.921	0.767	0.986	0.903	0.718	0.977	0.908	0.757	0.962	0.906	0.847	0.982	0.925	0.726	0.987	0.920	1.127	0.982
Recall	0.926	0.591	0.986	0.905	0.590	0.977	0.895	0.567	0.962	0.915	0.587	0.982	0.930	0.590	0.987	0.920	0.588	0.982
F1 score	0.921	0.455	0.986	0.904	0.454	0.977	0.852	0.750	0.960	0.900	0.546	0.981	0.925	0.453	0.987	0.906	0.332	0.981
True positive	0.926	0.591	0.986	0.905	0.590	0.977	0.895	0.567	0.962	0.915	0.587	0.982	0.930	0.590	0.987	0.920	0.588	0.982
False positive	0.055	0.410	0.010	0.055	0.410	0.015	0.102	0.432	0.032	0.074	0.413	0.017	0.054	0.410	0.009	0.075	0.412	0.018

Figure 5.12: Summary of ML models for all data types

Chapter 6

Conclusion and Future Work

Essentially, IoMT technology brings improvement in how patients' conditions are monitored and how doctors, nurses and other healthcare professionals are notified in the event of an emergency. It has brought about a drastic enhancement in remote patient monitoring. The aim of IoMT are that connected medical devices and sensors can constantly collect and analyze health data in real time, monitor health changes in patients, and increase the accuracy of a patient's diagnoses. It is capable of connecting entire networks of medical devices worldwide. However, the increasing rate of intrusions in the healthcare network has badly affected the security and privacy of patients and the healthcare sector at large. Also, their resource constraints e.g. limited battery power and limited processing power have reduced the efficiency of some security mechanisms like cryptography. One of the ways to address this is the use of IDS to provide secured transmission of data across the network. The security aspects of intrusion detection using machine learning approach have been considered in our paper. In conjunction with IoMT devices, machine learning can help build a more efficient IDS for medical organizations to support thousands of patients and manage sizeable amounts of data. Characteristics of ML techniques makes it possible to design IDS that have high detection rates and low false positive rates while the system adapt quickly to changing malicious behaviors.

In this paper, we have presented a novel Intrusion Detection System for detecting MitM and DoS attacks using ML methods. We have generated a specialized healthcare dataset for IoMT networks which was used to train six machine-learning algorithms: RF, KNN, SVM, ANN, J48, and Decision Table. Our dataset consists of 20 thousand records of normal, MitM and DoS attack packets. The port number and IP address can be removed from the features when considering a large dataset to avoid bias prediction. To build an efficient IDS, we propose the use of both patient's biometric data and network flow metrics. We have implemented our proposed solution using

MQTT protocol which is highly suitable for resource constrained devices like IoMT. It also provides the additional advantage of remotely monitoring the healthcare network. In this paper, the IoMT dataset was used to train and test machine learning using WEKA toolbox. The dataset contains normal and malicious traffic, and was used to obtain the experimental results. The attacks considered in this dataset were modification/insertion, data breach, ARP request, ICMP echo, TCP SYN, and UDP flood. Attacks were classified by a model built using cross-validation folds in which the original dataset splits into k equal parts (folds) where k equals 10. The results show that KNN is the best model to use for healthcare monitoring system as it gives the lowest execution time and generated an accuracy rate of 97.67%. The proposed IDS is based mainly on 8 parameters namely Accuracy, Execution time, Area under the ROC (AUC) score, Precision, Recall, F1 score, True Positive, and False Positive. Our IDS has a great effect for identifying and detecting the type of attacks and reducing the false alerts. We have implemented our proposed solution, and apply it in IoMT system, which is under MitM and DoS attacks, and are successfully detected. Results show that all ML methods used performed significantly better with combined features compared to using only one of the two features.

Although, the scope of our proposed model covers most of important points relevant to IoMT devices, there are few things which could further improve the scope of our project in the future. In our plan for future work, we aim to develop our intrusion detection system using Fuzzy Logic, which is known as one of the most powerful tools for reasoning under uncertainty for intrusion analysis. With Fuzzy Logic, we intend to effectively identify the intrusion activities in the network since it could give a reasonable conclusion in cases where situations are not explicitly defined in the rule based knowledge representation. Another improvement to enhance the methods' performance is by launching more advanced attacks like DDoS (Distributed Denial of Service) attack. This and other attacks can be launched by using multiple compromised sources to generate the attacks, and more efficient tools for traffic monitoring, statistics collection, visualization and processing. Furthermore, we can have a more robust and secure solution by integrating a private MQTT broker on the cloud.

Bibliography

[1] "Why the internet of medical things (iomt) will start to transform healthcare in 2018," Accessed 21-03-2021. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/?sh=fee4bd44a3ca

[2] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *Eurasip Journal on Information Security*, vol. 2020, no. 1, p. 8, dec 2020. [Online]. Available: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-020-00111-0

[3] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," *Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017*, no. 6, pp. 112–120, 2017.

[4] H. Sajjad and M. Arshad, "Evaluating Security Threats for each Layers of IoT System," no. October 2019, pp. 0–6, 2020.

[5] IBM Security and Ponemon Institute, "IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years," Tech. Rep., 2020. [Online]. Available: https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

[6] "Hackers stole personal, medication data of a quarter of Singaporeans - Help Net Security." [Online]. Available: https://www.helpnetsecurity.com/2018/07/23/singapore-healthcare-data-theft/

[7] "Machine learning - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Machine{_}learning

[8] I. H. Witten and E. Frank, *Credibility: Evaluating What's been Learned*, 2005.

[9] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 18, no. 2, p. 1153, 2016.

[10] K. Scarfone and P. Mell, "Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology," Tech. Rep.

[11] T. Ahmad, M. A. Anwar, and M. Haque, “Machine Learning Techniques for Intrusion Detection,” pp. 47–65, 2020.

[12] “Understanding Random Forest. How the Algorithm Works and Why it Is… | by Tony Yiu | Towards Data Science,” Accessed 2021-04-03. [Online]. Available: https://towardsdatascience.com/understanding-random-forest-58381e0602d2

[13] “K-Nearest Neighbors (KNN) Algorithm for Machine Learning | by Madison Schott | Capital One Tech | Medium,” Accessed 2021-04-02. [Online]. Available: https://medium.com/capital-one-tech/k-nearest-neighbors-knn-algorithm-for-machine-learning-e883219c8f26

[14] “k-nearest neighbors algorithm - Wikipedia,” Accessed 2021-04-02. [Online]. Available: https://en.wikipedia.org/wiki/K-nearest{_}neighbors{_}algorithm

[15] “Machine Learning: Types of Classification Algorithms,” Accessed 2021-04-03. [Online]. Available: https://serokell.io/blog/classification-algorithms

[16] “Artificial neural network - Wikipedia,” Accessed 2021-04-03. [Online]. Available: https://en.wikipedia.org/wiki/Artificial_neural_network

[17] “Comparative Study of J48, Naive Bayes and One-R Classification Technique for Credit Card Fraud Detection using WEKA,” Tech. Rep. 6, 2017.

[18] “Decision table - Wikipedia,” Accessed 2021-04-03. [Online]. Available: https://en.wikipedia.org/wiki/Decision{_}table

[19] F. Ahamed and F. Farid, “Applying internet of things and machine-learning for personalized healthcare: Issues and challenges,” *Proceedings - International Conference on Machine Learning and Data Engineering, iCMLDE 2018*, pp. 22–29, 2019.

[20] “82% IoT Devices of Health Providers, Vendors Targeted by Cyberattacks,” Accessed 2021-04-05. [Online]. Available: https://healthitsecurity.com/news/82-iot-devices-of-health-providers-vendors-targeted-by-cyberattacks

[21] R. Zaheer and S. Khan, “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” pp. 257–260, 2012.

[22] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, vol. 3, no. March, pp. 648–651, 2012.

[23] “Application Layer Protocols for IOT : IOT Part 11,” Accessed 2021-04-07. [Online]. Available: https://www.engineersgarage.com/tutorials/application-layer-protocols-for-iot-iot-part-11/

[24] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018.* Institute of Electrical and Electronics Engineers Inc., sep 2018, pp. 163–168.

[25] B. V. Santhosh Krishna and T. Gnanasekaran, "A systematic study of security issues in Internet-of-Things (IoT)," in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017.* Institute of Electrical and Electronics Engineers Inc., oct 2017, pp. 107–111.

[26] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IOT applications," in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017.* Institute of Electrical and Electronics Engineers Inc., oct 2017, pp. 477–480.

[27] S. R. Pokhrel, H. L. Vu, and A. L. Cricenti, "Adaptive Admission Control for IoT Applications in Home WiFi Networks," *IEEE Transactions on Mobile Computing*, vol. 19, no. 12, pp. 2731–2742, dec 2020.

[28] "(17) A Survey of the Self-Adaptive IoT Systems and a Compare and Analyze of IoT Using Self-Adaptive Concept." [Online]. Available: https://www.researchgate.net/publication/297650242_A_Survey_of_the_Self-Adaptive_IoT_Systems_and{_a_Compare_and_Analyze_of_IoT_Using_Self-Adaptive_Concept},note={{A}ccessed2021-04-07}

[29] "Internet of Things (IoT) Architecture: Key Layers and Components | AltexSoft," Accessed 2021-04-07. [Online]. Available: https://www.altexsoft.com/blog/iot-architecture-layers-components/

[30] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors (Switzerland)*, vol. 18, no. 9, sep 2018.

[31] "11 Internet of Things (IoT) Protocols You Need to Know About," Accessed 2021-04-08. [Online]. Available: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

[32] "Deep Dive into Zigbee for Home Automation," Accessed 2021-04-08. [Online]. Available: https://www.iotforall.com/deep-dive-into-zigbee-for-home-automation

[33] "What is Bluetooth Wireless Technology » Electronics Notes," Accessed 2021-04-08. [Online]. Available: https://www.electronics-notes.com/articles/connectivity/bluetooth/what-is-bluetooth-technology-basics-summary.php

[34] "Bluetooth Radio Versions | Bluetooth® Technology Website," Accessed 2021-04-08. [Online]. Available: https://www.bluetooth.com/learn-about-bluetooth/radio-versions/

[35] "LiFi - Future of IoT & Automation? Is WiFi under threat?" Accessed 2021-04-08. [Online]. Available: https://yourstory.com/mystory/lifi-the-future-of-iot-and-automation

[36] R. Kaur, "International Journal of Computer Science and Mobile Computing Light Fidelity (LI-FI)-A Comprehensive Study," Tech. Rep., 2014.

[37] R. Daidone, G. Dini, and M. Tiloca, "On experimentally evaluating the impact of security on IEEE 802.15.4 networks," in *2011 International Conference on Distributed Computing in Sensor Systems and Workshops, DCOSS'11*, 2011.

[38] F. Aftab, "Potentials and Challenges of Light Fidelity Based Indoor Communication System," *International Journal of New Computer Architectures and their Applications (IJNCAA)*, vol. 6, no. 3, pp. 92–102.

[39] P. Haripriya, "International Journal on Recent and Innovation Trends in Computing and Communication LI_FI Overview and Implementation in Medical Field ___________________________*****," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, no. 2, pp. 288–291, feb 2014.

[40] AL-mawee, "Privacy and Security Issues in IoT Healthcare Applications for the Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey Disabled Users a Survey Recommended Citation Recommended Citation," Tech. Rep., 2012.

[41] "A Systemic Approach for IoT Security | IEEE Conference Publication | IEEE Xplore," Accessed 2021-04-10. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.library.dal.ca/document/6569455

[42] "LTE and the Internet of Things," Accessed 2021-04-10. [Online]. Available: https://www.3gpp.org/news-events/1607-iot

[43] "4G LTE Advanced - What you need to know about LTE-A," Accessed 2021-04-10. [Online]. Available: https://www.4g.co.uk/4g-lte-advanced/

[44] "5G - Wikipedia," Accessed 2021-05-20. [Online]. Available: https://en.wikipedia.org/wiki/5G{#}Standards

[45] "(15) A survey on CIA triad for cloud storage services | Request PDF," Accessed 2021-04-10. [Online]. Available: https://www.researchgate.net/publication/311951056_A_survey_on_CIA_triad_for_cloud_storage_services

[46] "(No Title)," Accessed 2021-04-12. [Online]. Available: https://iotiran.com/media/k2/attachments/End_to_end_security_scheme_for_mobility_enabled_healthcare_Internet_of_Things.pdf

[47] A. Assiri and H. Almagwashi, "IoT Security and Privacy Issues," in *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*. Institute of Electrical and Electronics Engineers Inc., aug 2018.

[48] "Can I Trust the Data I See? | Proceedings of the Australasian Computer Science Week Multiconference," Accessed 2021-04-12. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3290688.3290731

[49] S. M. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[50] "The Internet of Things: A survey - ScienceDirect."

[51] F. R. Labs, "Connected Medical Device Security: A Deep Dive into Healthcare Networks," Tech. Rep.

[52] "Introduction to HL7 Standards | HL7 International," Accessed 2021-04-13. [Online]. Available: http://www.hl7.org/implement/standards/index.cfm?ref=nav

[53] "DICOM," Accessed 13-04-2021. [Online]. Available: Available:https://www.dicomstandard.org/

[54] "Point-of-Care Testing Standards Documents - CLSI Shop," Accessed 2021-04-13. [Online]. Available: https://clsi.org/standards/products/point-of-care-testing/documents/

[55] M. Wazid, A. K. Das, J. J. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182 459–182 476, 2019.

[56] "Intrusion Detection: A Survey | IEEE Conference Publication | IEEE Xplore," Accessed 2021-04-14. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.library.dal.ca/document/4693640

[57] "What is an Intrusion Detection System (IDS) and How Does it Work?" Accessed 2021-04-14. [Online]. Available: https://searchsecurity.techtarget.com/definition/intrusion-detection-system

[58] R. Mitchell and I.-R. Chen, "A survey of intrusion detection in wireless network applications," 2014.

[59] "A survey of intrusion detection systems in wireless sensor networks | IEEE Conference Publication | IEEE Xplore," Accessed 2021-04-14. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.library.dal.ca/document/7152200

[60] "Toward Practical Privacy-Preserving Processing Over Encrypted Data in IoT: An Assistive Healthcare Use Case," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 177–10 190, 2019.

[61] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[62] J. Zhang, H. Liu, and L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR," *IEEE Access*, vol. 8, pp. 38 995–39 012, 2020.

[63] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, pp. 95 956–95 977, 2020.

[64] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, and R. H. Deng, "Lightweight and Privacy-Aware Fine-Grained Access Control for IoT-Oriented Smart Health," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6566–6575, 2020.

[65] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3610–3617, aug 2018.

[66] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in iot," *IEEE Access*, vol. 7, pp. 135 632–135 649, 2019.

[67] V. J. Aski, S. Gupta, and B. Sarkar, "An authentication-centric multi-layered security model for data security in iot-enabled biomedical applications," *2019 IEEE 8th Global Conference on Consumer Electronics, GCCE 2019*, pp. 957–960, 2019.

[68] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks with Provable Security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[69] M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the internet of medical things," *2019 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2019*, pp. 1–4, 2019.

[70] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, pp. 25–30, 2016.

[71] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, “A forensics-by-design management framework for medical devices based on blockchain,” *Proceedings - 2019 IEEE World Congress on Services, SERVICES 2019*, pp. 35–40, 2019.

[72] G. Thamilarasu, A. Odesile, and A. Hoang, “An Intrusion Detection System for Internet of Medical Things,” *IEEE Access*, vol. 8, pp. 181 560–181 576, 2020.

[73] A. Bengag, O. Moussaoui, and M. Moussaoui, “A new IDS for detecting jamming attacks in WBAN,” *2019 3rd International Conference on Intelligent Computing in Data Sciences, ICDS 2019*, pp. 1–5, 2019.

[74] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, “Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study,” *IEEE Access*, vol. 8, pp. 106 576–106 584, 2020.

[75] “cu(1): Call up another system - Linux man page,” Accessed 2021-05-21. [Online]. Available: https://linux.die.net/man/1/cu

[76] “The GNU Awk User’s Guide,” Accessed 2021-05-21. [Online]. Available: https://www.gnu.org/software/gawk/manual/gawk.html

[77] “ECG patient monitor - PM6750 - Shanghai Berry Electronic Tech Co.,Ltd - RESP / TEMP / NIBP,” Accessed 2021-05-01. [Online]. Available: https://www.medicalexpo.com/prod/shanghai-berry-electronic-tech-co-ltd/product-122578-866819.html

[78] “How to read an Electrocardiogram (ECG). Part One: Basic principles of the ECG. The normal ECG,” Accessed 2021-05-02. [Online]. Available: http://www.southsudanmedicaljournal.com/archive/may-2010/how-to-read-an-electrocardiogram-ecg.-part-one-basic-principles-of-the-ecg.-the-normal-ecg.html

[79] “hexdump(1) - Linux man page,” Accessed 2021-05-21. [Online]. Available: https://linux.die.net/man/1/hexdump

[80] “od(1): dump files in octal/other formats - Linux man page,” Accessed 2021-05-21. [Online]. Available: https://linux.die.net/man/1/od

[81] “MQTT Client and Broker and MQTT Server and Connection Establishment Explained - MQTT Essentials: Part 3,” Accessed 2021-05-05. [Online]. Available: https://www.hivemq.com/blog/mqtt-essentials-part-3-client-broker-connection-establishment/

[82] U. Krčadinac, “Training and Testing,” Tech. Rep.

[83] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, “The WEKA data mining software,” *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 1, pp. 10–18, nov 2009.

[84] J. Li, “Detection of Ddos Attacks Based on Dense Neural Networks, Autoencoders and Pearson Correlation Coefficient,” no. April, p. 89, 2020.

[85] R. Taj, “A Machine Learning Framework for Host Based Intrusion Detection using System Call,” no. April, 2020.

[86] “Artificial Neural Network (ANN) Definition,” Accessed 2021-05-05. [Online]. Available: https://www.investopedia.com/terms/a/artificial-neural-networks-ann.asp

[87] “gnuplot homepage,” Accessed 2021-05-21. [Online]. Available: http://www.gnuplot.info/