TOWARDS SECURITY AND PRIVACY IN NETWORKED MEDICAL DEVICES AND ELECTRONIC HEALTHCARE SYSTEMS

A Thesis

presented to

the Faculty of California Polytechnic State University,

San Luis Obispo

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

Isabel Jellen

June 2020

COMMITTEE MEMBERSHIP

TITLE: Towards Security and Privacy in Networked Medical Devices and Electronic Healthcare Systems

AUTHOR: Isabel Jellen

DATE SUBMITTED: June 2020

COMMITTEE CHAIR: Joseph Callenes-Sloan, Ph.D.
Professor of Computer Engineering

COMMITTEE MEMBER: Dongfeng Fang, Ph.D.
Professor of Computer Science

COMMITTEE MEMBER: Bruce DeBruhl, Ph.D.
Professor of Computer Science

ABSTRACT

Towards Security and Privacy in Networked Medical Devices and Electronic Healthcare Systems

Isabel Jellen

E-health is a growing field which utilizes wireless sensor networks to enable access to effective and efficient healthcare services and provide patient monitoring to enable early detection and treatment of health conditions. Due to the proliferation of e-health systems, security and privacy have become critical issues in preventing data falsification, unauthorized access to the system, or eavesdropping on sensitive health data. Furthermore, due to the intrinsic limitations of many wireless medical devices, including low power and limited computational resources, security and device performance can be difficult to balance. Therefore, many current networked medical devices operate without basic security services such as authentication, authorization, and encryption.

In this work, we survey recent work on e-health security, including biometric approaches, proximity-based approaches, key management techniques, audit mechanisms, anomaly detection, external device methods, and lightweight encryption and key management protocols. We also survey the state-of-the art in e-health privacy, including techniques such as obfuscation, secret sharing, distributed data mining, authentication, access control, blockchain, anonymization, and cryptography. We then propose a comprehensive system model for e-health applications with consideration of battery capacity and computational ability of medical devices. A case study is presented to show that the proposed system model can support heterogeneous medical devices with varying power and resource constraints. The case study demonstrates that it is possible to significantly reduce the overhead for security on power-constrained devices based on the proposed system model.

ACKNOWLEDGMENTS

Thanks to:

- My parents, for their unwavering support throughout my college experience
- Those who have encouraged me, some maybe unknowingly, to pursue computer science, including friends, family, high school teachers, Cal Poly professors, and industry professionals I met through internships - to name a few, Sam Procopio, Eric VanBuren, Dr. Russell Westphal, Kurt Mammen, and Dhrumil Desai.
- Dr. Joseph Callenes-Sloan and Dr. Dongfeng (Phoenix) Fang for their expert advice and assistance in completing this thesis
- Andrew Guenther, for uploading this template

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Background

1.1.1 E-health background

In the past, medical records were stored in a paper repository consisting of clinical, research, administrative, and financial data. This approach had several limitations; for example, only one user at a time could access this paper-based repository, and any updates were performed manually. Most medical records departments were located in the basement of the institution due to the weight of the paper, and access was controlled by doors, locks, identification cards, and sign-out procedures [1]. In the past few decades, there has been a transformation in the quality and availability of healthcare services, due in part to the contributions of digitizing the industry. Recent developments have led to the adoption of Electronic Health (E-health) systems which are made possible in large part due to the large-scale adoption of communication technologies. Today, an electronic data management system has been adopted, which mitigates many of the limitations of the previous paper-based system. E-health is an emerging application of wireless networks which aims to minimize temporal, special, and monetary barriers to providing access to healthcare [2]. Recently, the term m-health was also introduced to refer to the use of mobile devices in patient monitoring and data transmission [3]. With advances in healthcare technologies and networked sensors, e-health has been used to deliver effective and efficient healthcare services as they provide medical staff with real-time remote access to patient data. Examples of e-health applications include remote monitoring of people with various chronic illnesses, patient-centric healthcare, and elderly monitoring [3]. However, the electronic storage of

healthcare records brings up key issues such as privacy and confidentiality, security, and data integrity and availability [1]. Some examples of potential attacks against e-health systems include data falsification, unauthorized access to the system, or eavesdropping on sensitive health data [4]. Furthermore, as a subsection of the healthcare industry, e-health must be especially vigilant about data privacy due to guidelines set forth by the Health Insurance Portability and Accountability Act (HIPAA), including protection of personal patient data [5]. Broadly, e-health security and privacy attempts to address two issues: security of medical data and privacy of the patient's data [6].

1.1.2 Wireless Sensor Networks Background

Wireless Sensor Networks (WSNs) are becoming a popular tool to deploy sensors and actuators in applications such as infrastructure, agriculture, smart home, healthcare, and military, recently becoming known as the Internet of Things (IoT). WSNs consist of spacially distributed sensor nodes which are mutually controlled by some given conditions. Nodes often communicate information which is collected from the surrounding environment [7]. Each sensor node is small and affordable in cost with limited computation power and memory.

In recent years, medical wireless sensors have been incorporated into patients' daily lives as an IoT healthcare platform [8]. As such, wireless sensor networks dominate the data collection layer of e-health systems, which are comprised of a body area network linked to a healthcare center via the patient's smartphone. Data is collected and stored across various platforms, from on-premises data stores to the cloud, with varying communication channels, such as SMS and e-mail, and transmission protocols, such as Bluetooth, WiFi, and Broadband [9]. The body area network consists of sensors and actuators which are interconnected often through short-range wireless communication such as IEEE 802.15.1/Bluetooth or IEEE 802.15.4/ZigBee [10].

1.1.3 Security and Privacy Background

Security generally relates to protecting sensitive data, whereas privacy safeguards a user's identity. In studying security and privacy, we first define a system model for the problem at hand, including protocols, data stores, and device types. Unique challenges presented by the system are taken into account, such as power constraints of certain devices in the system. Then, we outline vulnerabilities and threat models at each layer defined in the system model. In order to set goals for security solutions, we define security and privacy requirements and objectives. Three objectives that are commonly stated in security research are confidentiality, integrity, and availability. After compiling this necessary background information, we can then work on proposing security and privacy solutions.

1.2 E-health Security and Privacy

Data shared in a clinical setting, such as identification data, diagnoses, treatment and progress notes, and laboratory results, is considered confidential and must be protected under the HIPAA Privacy Rule [11]. This rule maintains that patient information should be released only with the permission of the patient except for certain treatment, payment, or administrative purposes, making data privacy a primary consideration in maintaining electronic healthcare data records [1]. While many researchers focus on electronic health privacy policies from American and European entities, privacy legislation with regards to e-health can be found in most developed countries [12]. Furthermore, healthcare data is becoming more valuable - to legitimate commercial entities interested in targeted marketing, to parties looking to illicitly obtain services, and to criminals selling an identity or using it to commit fraud [9].

There are several layers that must be considered in protecting e-health data, including the personal layer, transmission and communication layer, and services layer [9]. Four types of threats to an e-health system can be considered: threats to confidentiality, integrity, authentication, and availability. Several components of the system can be subject to each type of threat, including communication within the body area network, between the mobile device and network operator, within the operator's network, between the network operator and the cloud server, and between the server and the application [10]. Security of medical data is typically accomplished in the body area domain, while patient data privacy is mainly accomplished in the service domain [6].

There are several previous surveys related to e-health data security and privacy. In [9], the authors describe the data privacy and security concerns in e-health and discuss available tools to minimize risk of data compromise. In [13], the feasibility of adequately protecting against threats to privacy and security of electronic healthcare data is discussed. There are several systematic literature reviews on the privacy and security of e-health data [14] [15] [16] which review privacy and security challenges and future directions for e-health. There is also a survey on privacy solutions for the e-health cloud [17], but there have been significant developments in health data privacy since the date of publication of this paper. Although there is work surveying the privacy challenges of e-health, we did not find any current work which presented a comprehensive survey of current solutions to combat these privacy challenges.

1.3 Security with Consideration of Resource Limitations for Wireless Medical Devices

The final section in this thesis focuses on methods for securing e-health medical devices with consideration of their resource limitations. Traditional network security measures in-

clude encryption, authentication, and authorization of network communications. However, for devices which are severely power-constrained, these approaches may not be practical. In the case of implantable medical devices, a non-trivial challenge is whether power can be supplied sufficiently and continuously for the operation of the entire system [18]. Due to these constraints, many networked implantable medical devices on the market today operate without basic security defenses, making them vulnerable to cyber attacks [19][20]. Medtronic markets a line of implantable cardioverter defibrillators (ICDs) which support wireless programming and remote monitoring, such as the Medtronic Virtuoso [21]. The US Food and Drug Administration (FDA) issued a statement on March 21, 2019 to alert healthcare providers and patients on cybersecurity vulnerabilities identified in the Conexus Wireless Telemetry protocol [22]. As described in this statement, the Conexus protocol was found to contain vulnerabilities because it did not use encryption, authentication, or authorization. According to the Medtronic security bulletin, the Conexus protocol allows remote transmission of data from the cardiac device to a specified clinic, display of device information in real time for physicians, and wireless programming of device settings.

Although this is just one example of the security vulnerabilities which exist in implantable medical devices, the lack of basic security measures such as encryption, authentication, and authorization is not uncommon in networked implantable medical devices due to resource and power constraints. Furthermore, security vulnerabilities in these life-critical systems could lead to not only the compromise of sensitive personal data but also potentially to injury or death. There is some research work related to constrain of medical devices [23, 22], attack vectors and threats for medical devices [24, 25], lightweight encryption and key management for medical devices [26, 27], and external hardware for medical device security [28, 29, 30]. However, most current work does not consider the heterogeneous system model for e-health security. Therefore, our final contribution will be to propose an e-health system model with consideration of the resource limitations of wireless medical

devices and provide a case study to show that this system model supports medical devices with varying power and resource constraints.

1.4 Major Contributions and Organization

There are several contributions of this thesis, including:

- A comprehensive system model for e-health
- A survey of the state-of-the-art in e-health security and privacy
- An e-health system model which considers varying battery capacity and computational ability for medical devices
- A case study which demonstrates that the proposed system model can support heterogeneous medical devices, showing that it is possible to reduce the computational overhead to provide security on power-constrained devices in the system

The remainder of this thesis is structured as follows:

1. In Chapter 2, we present a survey of the state-of-the-art in e-health security, including a comprehensive system model, an outline of attack models, a description of security objectives, and a survey of current solutions.
2. In Chapter 3, we present a survey of recent work in e-health privacy, including an outline of challenges and threats, a description of privacy objectives, and a survey of current solutions.

3. In Chapter 4, we propose a comprehensive system model for e-health applications with consideration of battery capacity and computational ability of medical devices. A case study is presented to show that the proposed system model can support heterogeneous medical devices with varying power and resource constraints.

4. Finally, in Chapter 5, we present conclusions and ideas for future works.

Chapter 2

E-HEALTH SECURITY

2.1 E-Health System Model

An e-health system is one which electronically exchanges healthcare information from patient to provider and is comprised of a body area network linked to a healthcare center (often via the user's smartphone).

2.1.1 System Architecture

There are multiple layers to consider in a e-health system, including the perception layer, network layer, data processing layer, and application layer. The layers considered in this system are shown in Fig. 2.1.

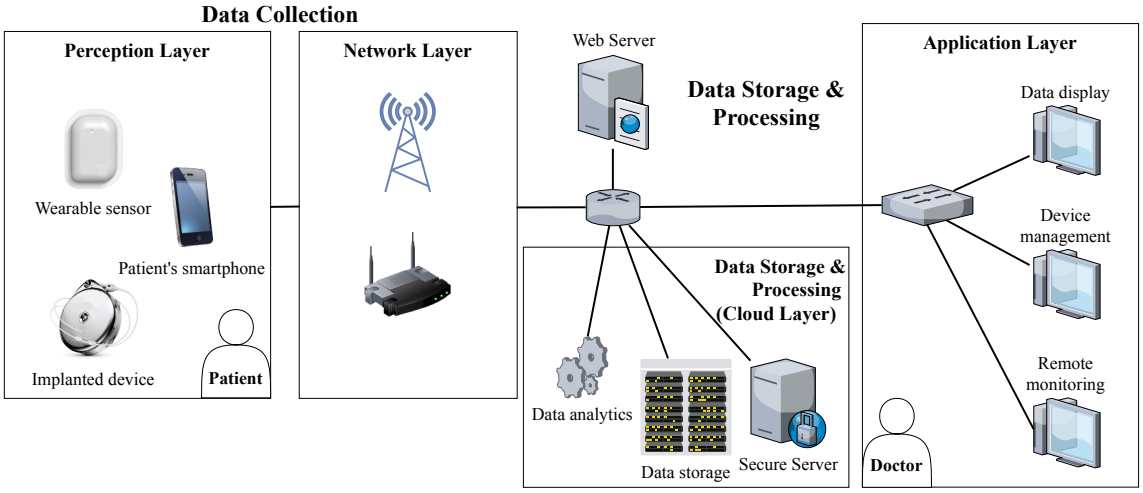

Figure 2.1: E-health overall system architecture is shown.

The system is comprised of four major network layers [31]:

1. Body area network (BAN) or Perception Layer: Body sensors and smart mobile device. Often, protocols such as Bluetooth or ZigBee are used in this layer.
2. Personal area network (PAN) or Network Layer: Connects the BAN with the remainder of the system via WiFi or cellular networks
3. Wide area network (WAN) or Data Processing Layer: Internet connection to data processing server layer, which handles analytics, data storage, and providing a secure server
4. Application Layer: Back-end to user and physician software applications

The perception layer, or body area network (BAN), consists of sensors and actuators which serve to collect physiological data and provide therapy. Devices within the perception layer of e-health systems include wearable devices as well as connected implanted devices. Often, protocols such as Bluetooth or ZigBee are used in this layer.

The network layer, or personal area network (PAN), serves to connect the perception layer with the remainder of the system through a WiFi connection or cellular networks. In many cases, the user's smartphone is used to provide this link, often through an app developed for this purpose by the healthcare provider.

In the wide area network (WAN) layer, an internet connection provides a link between the PAN layer and the data processing server layer. The data processing layer serves several functions, such as data analytics, data storage, and providing a secure server. Data analytics may include statistical or machine learning models to provide insights on patient data trends, anomalies, or other metrics.

In the application layer, multiple functionalities are implemented, such as remote control of therapy settings, data display, device management, and remote patient monitoring.

2.1.2 System Constraints

There are a few notable constraints on e-health medical devices, including their small size, processing limitations, and non-rechargeable battery [32].

1. Size is a limitation of medical devices because they often need to be deployed in or on the user's body. For implantable devices, larger devices are more likely to be rejected by the immune system. For wearable devices, users are unlikely to wear a device that is large and inconvenient.

2. Processing power in medical devices is also typically low, in part due to size and cost restrictions.

3. Battery life in medical devices can last up to ten years; however, security protocols such as cryptography, machine learning approaches, and hashing require significant power which could quickly drain the battery. If the battery is exhausted, the whole device needs to be replaced, which can be especially challenging for implantable devices. Communication transmissions themselves cause significant power consumption, so low-power techniques must be used for communications [32].

2.2 Attack Models and Security Objectives

From the network model shown in the previous section, several attack vectors can be identified [33]:

1. Medical device software, hardware, or firmware vulnerabilities
2. Protocol vulnerabilities (Bluetooth, BLE, ZigBee, WiFi, Cellular, etc.)
3. Non-compliant or over-privileged smartphone apps
4. Inadequate protection of data stored at the gateway (e.g. lack of encryption, access control, authentication, or inappropriate policy)

Threats to medical devices in an e-health can be classified into three broad categories: confidentiality, integrity, and availability, as shown in Fig. 2.2.

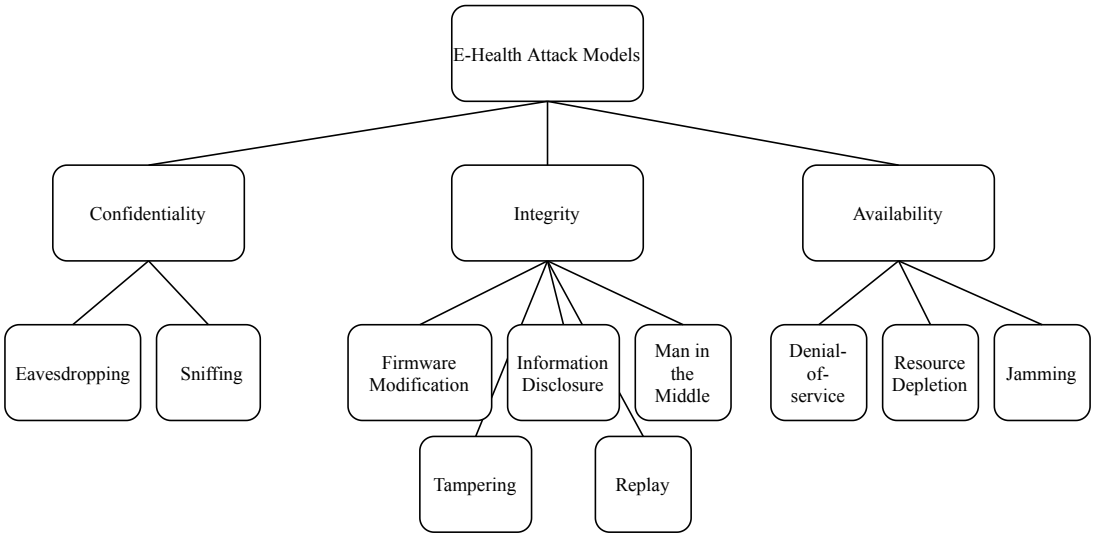

Figure 2.2: Attack models applicable to e-health are displayed and classified into the three major security objectives, confidentiality, integrity, and availability.

2.2.1 Confidentiality

Threats to confidentiality are eavesdropping attacks in which the attacker gains unauthorized access to sensitive information. This may include patient data or credentials. This type of attack is targeted mainly at the network layer and can be prevented using encryption of exchanged data and identification and authorization mechanisms for incoming network traffic [34]. The main attacks against confidentiality are eavesdropping and sniffing. Eavesdropping is real-time interception of a user's personal information by an adversary. Sniffing is focused on traffic analysis to obtain sensitive data such as credentials and MAC addresses. Eavesdropping and sniffing attacks utilize spyware, a universal software radio peripheral, or traffic analysis and exploit weak or non-existent encryption algorithms [33]. The privacy of healthcare data in patient identity is especially important due to the need to comply with legislation such as HIPAA, so data confidentiality is of paramount importance in e-health systems.

2.2.2 Integrity

In threats to confidentiality, the attacker tampers with sensitive information. This may include modifying medical device therapy settings, deleting stored medical data, drifting the clock to make timestamps invalid or misleading, or even disabling the device altogether [35]. In a firmware modification attack, an adversary modifies a program stored in non-volatile memory that controls hardware of the device. Researchers have demonstrated firmware modification attacks on medical devices which often use reverse engineering and exploit insufficient of input validation, encryption, or authentication. Another prevalent attack on medical devices is information disclosure, in which sensitive data is exposed by an unauthorized entity. Additionally, an adversary can perform a man-in-the-middle attack by intercepting the communication between two legitimate parties. Information dis-

closure, unauthorized access, and man-in-the-middle attacks have also been implemented in e-health applications by exploiting weak authentication, encryption, and message integrity mechanisms. Tampering and modification attacks have also been implemented on implantable and wearable medical devices using reverse engineering and weak channel exploitation. Tampering and modification attacks alter data without proper authorization. Replay attacks can also be used in the context of medical devices in order to obtain valid packet data, intending to corrupt or impersonate it. [33].

2.2.3 Availability

Threats to availability include attacks (often called denial-of-service attacks) where the adversary acts to deny services to legitimate users. Motivations may include preventing a medical device from collecting or transmitting data, or preventing the device from receiving configuration. Denial-of-service attacks are typically either implemented as flood attacks or buffer overflow attacks. Flood attacks send an overwhelming number of packets to a given device, saturating the target device. Buffer overflow attacks use a memory buffer overflow to cause the target device to consume all available memory or CPU time. Denial-of-service, resource depletion, and jamming attacks have been demonstrated on medical devices by using a universal software radio peripheral or exploiting communication channels with weak encryption mechanisms or bombarding the device with requests. Due to the resource-constrained nature of many networked medical devices, the battery of these devices could be easily drained by launching such an attack [33].

2.3 Security Vulnerabilities

Medical devices on the market today often have severe security vulnerabilities for several reasons. First, implantable and wearable devices are power-constrained, so they cannot

afford the energy expense of additional security. Secondly, the primary function of medical devices, which is providing medical treatment or monitoring, can be life-critical, so many medical device manufacturers argue that proper function of the device should be considered before security. When manufacturers are trying to balance software and hardware functionalities, low power consumption, and low cost, security often falls to the wayside. Some medical device manufacturers use proprietary protocols in their networked medical devices to save on cost and offer increased customization. However, these proprietary protocols often sacrifice security in favor of lowering energy requirements or cost. For example, a proprietary protocol utilized in many networked devices developed by Medtronic was recently shown to lack basic encryption and authentication services [22]. Security vulnerabilities that have been exploited in recent medical device security research in implementing attacks against confidentiality include [33]:

- Lack of encryption
- Insecure key exchange
- Sending credentials and sensitive information in cleartext

Vulnerabilities exploited for attacks against integrity include:

- Missing input validation checks
- Weak access control and authentication mechanisms
- Absence of read / write protection in device firmware

Vulnerabilities exploited for attacks against availability include:

- Absence of traffic restriction
- Absence of traffic analysis

2.4 Current Solutions

Several approaches have been proposed to increase security in light of the unique challenges of e-health systems, as shown in Table 2.1.

Table 2.1: Security Solutions for Demonstrated Attacks

Security Solution	Approaches	Attacks Addressed
Biometric Approaches	Biometric authentication, key generation from biometrics	Eavesdropping, Man-in-the-middle
Distance / Proximity Based Approaches	Sound detection through piezoelectric element, Near Field Communication (NFC) tag	Eavesdropping, Replay
Key Management	Symmetric key cryptography, Public (asymmetric) key cryptography	Denial of service, Eavesdropping, Man-in-the-middle, Replay
Audit Mechanisms	Maintenance and alerting on device audit logs	Non-repudiation
Anomaly Detection	SVMs to classify network activities	Internal attacks, Resource depletion, Malicious communication
External device methods	IMD Guardian - external device using electrocardiogram signals, IMD Shield - full duplex radio device with receiver and jamming antenna, Cloaker - external device which shares master key to authenticate device and caregiver	Eavesdropping, Device capture
Lightweight encryption and key management techniques	Vibration-based key exchange protocols	Eavesdropping, Man-in-the-middle

2.4.1 Access Control

2.4.1.1 Biometric Authentication

Biometric authentication measures unique, verifiable physiologic characteristics and searches against samples stored in the system using screening, scanning, and feature extraction. First, the reference image is chosen from the images captured as the clearest image. A discriminative bit set is acquired from the image, and hamming distance is used as a distance metric to verify the biometric [32]. This approach requires relatively low overhead, but there is a security concern that storing biometrics in the system is similar to storing a master key in the system. Bio-cryptographic key management protocols have also been proposed, where unique physiological features such as Inter Pulse Interval (IPI) are used to generate random cryptographic keys. In such methods, the finite monotonic increasing sequence generation mechanisms and Hamming Distance can be used to extract bits from physiological signals with a high degree of entropy. These random bit sequences can be used as cryptographic keys for secure data exchange [36].

2.4.1.2 Distance-based approaches

Distance-based approaches to security in medical devices have been proposed, where access is granted through touch or close proximity. For example, the work presented in [37] detects sound emitted by the medical device through an implanted piezoelectric circuit element in its access control scheme. In [38], a Near Field Communication (NFC) approach is used for access control to patient information in the medical device. In this method, an NFC tag is implanted into the patient's body, enabling communication with a medical practitioner through the use of a smart phone. Such approaches avoid the need for cryptographic techniques, which place strain on battery life.

2.4.1.3 Key Management

Symmetric and public key techniques can be used to manage cryptographic keys used in encryption and message authentication. In symmetric techniques, a secret key is shared between only the trusted devices and personnel. Public key techniques utilize a public key, which is made public, and a secret key which is used as a digital signature. Symmetric key techniques are generally preferred for medical device applications as they are less costly in terms of computational complexity and power consumption. Asymmetric methods often utilize complex circuits and high data exchange rates and communication before granting access, increasing the power consumption of the device [32].

2.4.2 Auditing and Anomaly Detection

Audit logs are maintained in many medical devices in order to keep a record of the patient's health history and conduct of the device over a particular time interval. However, memory limitations in medical devices could lead to overflowed audit logs, making the device vulnerable to attacks. One approach to mitigate such risks is alerting the provider upon completion of memory storage [39] or overwriting previous data which is no longer relevant. Anomaly detection approaches have also been proposed, such as the approach proposed in [40], which uses unsupervised support vector machine (SVM) methods for detecting resource depletion attacks. Medical device access patterns specific to a given patient are used to train the SVM, with access information being comprised of five fields: reader action, time interval, location, time, and date of use. This information is fed into linear and non-linear SVMs for learning and classification. In this experiment, the linear and non-linear SVMs produced accuracies of 90% and 97%, respectively, for classification of resource depletion attacks. One concern about machine learning approaches is the processing power it takes to train and deploy such algorithms.

2.4.3 External Hardware Approaches

Several external device approaches have been proposed to improve the security of medical devices, such as Cloaker [28], IMD Guard [29], and IMD Shield [30]. These external devices generally aim to increase access control to the device in normal operation but remove barriers to access in health emergencies. The Cloaker device is an external device worn by the patient to ensure security of the medical device (completely ignoring all authentication requests) when worn and give open access when not worn. The idea is that the Cloaker device can be removed in a health emergency situation and the medical device will respond to all authentication requests. IMD Guard is mechanism which uses an external device called the Guardian. This approach is used with cardiovascular devices such as implantable cardioverter-defibrillators, pacemakers, and electrocardiogram sensors. The Guardian facilitates interactions between the healthcare provider and medical device in order to provide security in normal situations but provide access in case of emergency. A challenge-response technique where the device sends challenges at different time intervals is used to enter the emergency mode. The medical device programmer is authenticated by verifying the signature of the device, issuing temporary session keys. The patient's ECG signals are used for key sharing between the device and the Guardian. One vulnerability of the Guardian approach is that it is vulnerable to man-in-the-middle attacks. The third external device, IMD shield, is a full-duplex radio device consisting of a receiver and jamming antenna. The receiving antenna obtains and deciphers signals, and the jamming antenna transfers an arbitrary flag to prevent eavesdropping by blocking interception of transmissions from the medical device. One vulnerability of this approach is that IMD Shield commands do not remain confidential when the commands are sent from the caregiver to the medical device. Furthermore, this device does not comply with FDA regulations as jamming interferes with other radio frequency devices, so this is not a feasible solution.

2.4.4 Lightweight Encryption and Key Management

Vibration-based key exchange protocols have been proposed as lightweight security for medical devices [41]. In this scheme, vibrations are initially received by measuring vibrations of an accelerometer. Low frequency noise from action of the patient is then removed using a high pass filter, and the RF module is activated in the case that a high-frequency signal is perceived. Once the RF module is activated, the symmetric key can be shared between devices. The key is produced by the first and modified into a vibration signal. Once this signal is received, it is transformed back into a bit string key using a two-feature On-Off Keying (OOK) demodulation mechanism. The major limitation of this approach is that an adversary may be able to extract keys from vibration signals, which are acoustic and electromagnetic waves that could potentially be captured [33].

2.5 Conclusions: E-health Security

This survey provided a system model along with attack models and security objectives. We outlined common security vulnerabilities in medical devices, then surveyed current solutions which address the given attack models.

Based on this survey, future directions for research are suggested as follows:

- Address security vulnerabilities present in legacy medical devices deployed in many real-world systems.
- Ensure data and message integrity without significant additional computational overhead.
- Develop more secure lightweight cryptographic and authentication protocols.

- Implement proper firmware integrity check mechanisms to prevent firmware modification.
- Design a legitimate external eavesdropper that detects malicious network traffic using machine learning techniques. This will increase rates of attack detection without consuming power of the medical device.
- Dynamically recover the system after detecting attack vulnerability by changing the network configuration.
- Propose a standard communication protocol for body area network communication.

There is a lot of work still be done to address wireless security and privacy concerns in the field of e-health, especially due to the sensitive nature of the data being transmitted and the unique constraints of medical devices. E-health promises a way to increase access to healthcare and has been steadily growing in popularity, so it is important to secure this platform as we move into the future.

Chapter 3

E-HEALTH PRIVACY

3.1 System Model

Here, we split the e-health system model as shown in Fig. 2.1, which includes the perception layer, network layer, cloud layer, and application layer into two primary components: data collection and data storage and processing.

The perception layer includes networked medical devices, including wearable sensors, actuators, and implantable devices, in addition to smart devices which act as a gateway between the perception layer and network layer. Patients' health data transmitted in this layer may include ECG, fetal monitors, temperature, or blood glucose levels [8]. Protocols such as Bluetooth, WiFi, ZigBee, and cellular are commonly used in the perception and network layers, which together comprise the data collection component of the e-health system. The data storage and processing layer commonly includes the cloud layer, including data storage, analytics, and processing. This component is often implemented as a Software as a Service (SaaS) architecture.

3.2 E-health Privacy Challenges

3.2.1 Data Collection: Vulnerabilities and Threat Models

In the data collection stage, there are two primary locations where data privacy can be compromised: at the perception layer, or at the network layer by a third-party service provider (TSP) or communication service provider (CSP). In a medical data sharing framework,

parties involved include patients, researchers, wearable device providers, and data brokers. Patients typically trust hospitals and health service providers, but not necessarily the third parties that are involved [42]. Because of this, it is important to properly identify trusted and untrusted third parties in an e-health data collection system.

There are several potential threats to data privacy at perception layer. Due to the ubiquity and lack of standardization of IoT devices in today's world, some medical sensors consistently provide protected data, while others may be prone to attacks such as eavesdropping [43]. Wearable medical devices are small in size, so therefore they have smaller battery sizes that need to be constantly charged. Traditional cryptographic algorithms need more power than allowed by many wearable devices, underscoring the need for low-power privacy defenses [44]. The data stored in wearable devices are often not encrypted, ant the devices do not have any password protection, pin or biometric security, making wearable devices weak in tamper-resistance [44]. Furthermore, a user may have other IoT devices in their home which could interfere with the medical sensor devices if they are under similar networks [43]. Another challenge of data collection in e-health is the reliability and accuracy of information collected by the patient themselves [45]

It is not only medical sensors that collect sensitive data in the healthcare system; in [46], researchers demonstrate that RFID (Radio Frequency IDentification) can be used in healthcare to efficiently track hospital supplies, medical equipment, medications and patients. However, the prospect of wide spread use of RFID tags in healthcare has raised questions regarding privacy, because RFID data in transit can easily be intercepted and potentially used to trace personal health information, clinical history and financial information of the user.

Regardless of whether the data transmitted by sensors in the IoT healthcare system is protected or not, another attack surface is presented at the network layer, in data transmission from the patient to the cloud server by the communication service provider (CSP), which

may not be fully trusted [43]. Sensitive physiological data sent can be sent over open wireless channels, enabling threats such as eavesdropping, impersonation, data integrity, data breach, collusion, and so on [47].

Threat models of the data collection layer in an e-health system are detailed in [8] as follows:

1. Collusion: In this attack, an IoT medical device purposely maintains connections with an outsider, who may be motivated to gain sensitive information about the patient from the healthcare system

2. Eavesdropping: In an eavesdropping attack, health data transmitted by a medical sensing device can be sniffed, resulting in loss of data and potentially identity privacy.

3. Impersonation: Here, an attacker plays the role of a trusted party by the medical sensor, potentially permitting the attacker access to the health data, database, and network resources.

4. Data Leakage: In this attack, health data is transmitted from the healthcare system to an unauthorized external destination.

3.2.2 Data Storage and Processing: Vulnerabilities and Threats

Data stored in an e-health system can be referred to as the Electronic Health Record (EHR) or Electronic Medical Record (EMR). Due to the huge volume and complexity of healthcare data, it is infeasible to manage this data using traditional software or hardware approaches. As a result, many institutions are moving towards cloud-based systems. A challenge which is unique to cloud-based systems is shared tenancy, where multiple parties share the same physical hardware [48]. Furthermore, the introduction of a cloud-based data storage system requires some amount of trust in the cloud service provider.

One of the challenges in the data storage and processing layer of the IoT healthcare system is ensuring that only authorized parties have access to store and retrieve data [49]. It is important to remember that the patient should always maintain the role of data owner, whereas hospital staff is a data user [50]. Access control models can be effective for external attacks, but are generally ineffective against internal attackers as they are likely to be authorized to access the data [45].

In data storage, we must consider the scenario that the storage system is attacked and the data stolen. In this case, the attacker should not be able to determine the content of the data, which can be achieved by encryption [49]. When stored data is encrypted, if the system loses control over the data, patients will be accountable for their data as they will control the encryption keys [51]. However, encryption of data limits the searchability of the data: healthcare providers have to decrypt the data prior to searching on the decrypted data, resulting in increased time and cost for the data retrieval and processing [45].

Furthermore, in the event of data compromise, the attacker should not be able to gain the identity of the patient [52]. The patient's permanent identifier should not be stored with their personal health information; rather, a temporary identifier should be used to make data untraceable to its original owner [52]. Another consideration is the need to be able to process healthcare without revealing patient identity. There are several motivations for being able to process large amounts of clinical data while preserving patient anonymity, such as training machine learning models [53] [54], better understanding of patterns and trends in public health and disease [55], diagnosis diseases and find treatments [56], and per-patient data sharing between healthcare institutions [57]. Anonymization can be used to process large amounts of patient data while being able to preserve identity privacy; however, such techniques may present tradeoffs with searchability, efficiency, and resulting model quality [56].

Several threats to the data storage and processing layers of the e-health system are summarized as follows [58]:

1. Spoofing: An adversary can gain access to medical data through forged credentials.
2. Malicious Insiders: Doctors who are the authorized users of e-health records can share this data with unauthorized pharmacies and laboratories in acts of unauthorized information disclosure.
3. Data Leakage: In a data leak, if not properly anonymized and encrypted, an attacker can gain access to the identity and / or personal health information of users.
4. Repudiation: Each activity must be monitored and logged with entity details so that an entity cannot deny modifying data.

3.3 Security and Privacy Requirements and Objectives

The HIPAA Privacy Rule [11] governs general policy decisions on collection, storage and processing of healthcare data, maintaining that data shared in a clinical setting, such as the patient's identification, diagnoses, treatment, and laboratory results, must only be released with the explicit permission of the patient. In part because of such policies in the healthcare system, and additionally to protect very sensitive patient data, security and privacy requirements must be more stringent in e-health than in some other IoT or cloud computing systems. All layers of the e-health system share common underlying security and privacy goals [42], including:

- Accuracy: Health-related data often is characterized by a certain accuracy which must be preserved by the e-health system
- Authenticity: The source of data must be able to be accurately verified

- Confidentiality: Patient data and identity confidentiality must be preserved throughout the e-health system
- Freshness: Monitoring of certain health conditions may require short response times following data collection
- Availability: The data collection and processing systems must maintain availability
- Integrity: The system should be able to detect tampering and be tamper-resistant

3.3.1 Data Collection

At the data collection layer of the e-health system, it must be ensured that if data is compromised on a physical node on a multi-hop system or at the communication service provider level, the confidentiality of the user's data and identity must be maintained. Since data collected may be sent to the cloud over open wireless channels, very little trust can be put in the entities involved in transmitting data to the cloud [47] [8]. However, in order to provide end-to-end mechanisms for ensuring security and privacy, researchers often assume that the data is collected by certified and trusted devices [42]. Since users may often be collecting data themselves in an e-health model, checks may need to be put in place in order to ensure that the data is collected by the device as intended and is as accurate as possible [45].

Power, memory, and size constraints on networked medical devices also must be considered in designing security solutions for the data collection layer [44]. Availability is also a concern for data collection in an e-health system, since data must be able to be collected continuously and uploaded to the cloud for processing in real time for many applications [45].

3.3.2 Data Storage and Processing

The patient is considered the owner of their health data according to the HIPAA Privacy Rule [11]; therefore, they should have the ability to grant, deny, or delegate access to their own data [59] [42]. Other parties, such as healthcare administrators, healthcare practitioners, and patient family members may also need access to the patient's data [59]. Each of these parties should only have access to the data they need to perform their job. Furthermore, when a user requests access to a patient's data, they must have a valid credentials which are validated by an authentication server, which grants the proper access. It also should be noted that in the case of an acute health emergency, immediate access to the necessary patient data should be granted to an available healthcare practitioner [59].

Many recent works in data storage for healthcare systems require that the confidentiality of the user's data and identity is maintained even if an attacker gains access to the data or any of the cloud servers in the e-health system [43]. In some research, decentralization of the database is added as a security requirement in order to avoid a single point of failure as is seen in centralized systems [45] [51] [49] [53].

For data processing, there must be a method to anonymize data in order for patient data to be able to be shared for purposes such as research investigations without revealing the associated patient identity [60] [61] [58].

3.4 E-Health Privacy Solutions

Many e-health privacy solutions proposed in existing research primarily focus on one layer of the e-health system: data collection, storage, or processing. Research can be further classified by the general solution type proposed, listed below:

- Obfuscation
- Secret sharing
- Distributed data mining
- Authentication
- Access control
- Blockchain
- Anonymization
- Cryptography

3.4.1 Obfuscation

Obfuscation techniques in e-health privacy are focused on the data collection layer, disguising the true use of a medical device in order to combat attacks such as traffic analysis. For example, in [62], physiologic parameters are embedded into a message from a cover device. In this implementation, the cover device is intended to not be associated with serious medical conditions; an example for a cover device might be an IoT light bulb. In order to select the cover device, the system scans for nearby devices in order to produce a realistic device type. Some methods suggested by [62] to embed physiological parameters

into messages include buffering physiological data prior to transmission, using a packet length associated with the physiological data, or multiplexing the physiological data across multiple cover devices.

Obfuscation can also be used at the cloud data storage layer by using decoy techniques as in [48]. Also called ”fog computing,” these methods create decoy information and locate it beside the real information in the cloud to hide the true owner of the data.

3.4.2 Secret Sharing

Secret sharing methods are used at the cloud layer in order to preserve the privacy of stored patient data. In a secret sharing scheme, a secret is encoded into a number of shares, which are distributed across servers at the cloud layer, each cloud server holding one share of the secret [47]. When enough secret shares are combined, the secret can be reconstructed [43]. In e-health applications, the ”secret” can be considered to be the sensitive patient data being stored on cloud servers. Several secret sharing schemes exist, including Shamir and Blakley’s [63] [64], where the size of the share is 1/m the size of the secret, where m is the number of blocks in the secret. One major drawback of these methods is heavy computation cost, so some research has been done in the context of e-health secret sharing to propose a scheme with lower computation cost. One such method is based on Slepian-Wolf coding, which achieves optimal share size using binning [47].

3.4.3 Distributed Data Mining

While secret sharing helps preserve the privacy of stored data, distributed data mining techniques can help preserve the privacy of data being processed. This can allow parties to acquire knowledge from healthcare data without gaining access to sensitive patient data. One example of such a method is an adaptive distributed privacy-preserving data mining

technique based on an ensemble strategy [53]. Another approach is a distributed learning method which keeps all data within the originating institution [65].

3.4.4 Authentication

Some research has been pursued in privacy-preserving authentication techniques for e-health, which mainly concerns access to stored patient data. In [59], Public Key Infrastructure (PKI) is used for authentication, where the authentication server validates the user's digital certificate. This ensures that only users with a valid certificate are granted access to a patient's data. Work has also been done in authentication for RFID-based systems in e-health, where authentication uses an anonymous protocol to disclose less information than existing RFID authentication schemes [46]. In this scheme, no sensitive information is leaked to the adversary even if a tag's information is read without the knowledge or consent of the owner.

3.4.5 Access Control

Access control is the mechanism that enables legitimate parties to access stored data without allowing an attacker to view or edit the data. The most standard form of access control in existing literature and industry practice is role-based access control. Privacy-aware versions of role-based access control by using group-based access control in order to preserve sender anonymity [46]. Researchers in [59] propose an attribute-based access control model which grants the proper access level based on resource attributes, subject attributes, and environmental attributes.

3.4.6 Blockchain

As decentralization has promised privacy preservation, there has been a lot of recent research on blockchain for e-health, which leverages its properties of decentralization to ensure accountability, integrity, and privacy. Blockchain has been demonstrated in the financial field as a trusted, auditable data storage mechanism, which is accomplished by using a decentralized network of peers and a public ledger. Blockchain is a growing list of records (or "blocks") which are cryptographically linked, where blocks are distributed across multiple nodes of a cloud infrastructure and are not centrally stored. In e-health applications, each block would contain a timestamp of its creation, a hash of the previous block and transaction data, and patient healthcare data [45]. Once in the blockchain, data is publicly accessible, so some research has been done on encrypting and obfuscating data before inserting it into the blockchain [51] [49]. One paper uses a sidechain and a mainchain to disassociate the identity of the patient with their health data [52]. In this approach, the sidechain is a private chain which stores the identity of the patient, and the mainchain is a public chain which stores the patient's data with a temporary identifier. Permissioned blockchains can also be provisioned to preserve privacy in e-health applications by using channel formulation schemes and membership service supported by blockchain. There is also research that suggests that blockchain-based solutions could enable an untrusted third party to process a patient's data without violating patient privacy [55].

3.4.7 Anonymization

There has been significant research in the use of anonymization to preserve patient privacy in e-health systems while being able to mine the data for research purposes. K-anonymity can be used to hide the origin of the dataset and identity of the patient by using supression and generalization [61]. Another tool for anonymization of healthcare data was proposed

which uses techniques such as including fake data and replacing characters by random numbers and letters [66]. Another approach to acheive privacy-preserving data publishing is detailed in [60], where anonymization is achieved through data publishers who act as a middleman between the data owner and recipient to ensure that the privacy of the data owner is preserved throughout the transaction. The authors of [58] list several techniques that can be used to anonymize data, including generalization, suppression, and pseudonymization. Generalization is a widely used anonymization approach which uses predefined hierarchies or values; suppression is a version of generalization in which values are replaced with '*', and pseudonymization is a version which replaces values with pseudonyms.

3.4.8 Cryptography

Cryptography approaches have been proposed for privacy preservation both for stored data and data in transit to the cloud following data collection. For encrypting stored data, [48] proposes a three-party one-round authenticated key agreement protocol based on the bilinear pairing cryptography that can generate a session key among the participants and communicate among them securely.

Encrypting data in transit from the data collection layer is more complicated since medical devices are often power, CPU, and memory constrained, making traditional cryptographic approaches often impractical. To this end, one paper proposes a lightweight field programmable gate array (FPGA) hardware-based cipher algorithm for use in e-health data collection [8].

3.5 Conclusions: E-health Privacy

In this paper, we survey privacy in e-health applications. First, we present a comprehensive e-health system model, dividing the system into two main sections: data collection, and data storage and processing. Then, we present challenges, vulnerabilites, and threats based on this system model. We then define security and privacy requirements and objectives, including goals such as accuracy, authenticity, confidentiality, freshness, availability, and integrity. Finally, we survey the state-of-the-art in e-health privacy, detailing solutions such as obfuscation, secret sharing, distributed data mining, authentication, access control, blockchain, anonymization, and cryptography.

It seems that an important step for future work in e-health privacy would be to further investigate the policy side of the problem. Although current regulations require compliance with the HIPAA privacy laws, these are fairly vague and do not provide specifics for e-health systems. Also, it would be helpful to have more research in patient-centric privacy, allowing patients to specify who can have what level of access to their records. Finally, as wearable and implantable medical sensors increasingly become an important part of e-health systems, more work should be done on privacy for these data collection devices, which may be limited in power and memory and require creative approaches to preserve privacy without depleting their resources.

Chapter 4

HETEROGENEOUS SYSTEM MODEL FOR SECURITY IN E-HEALTH APPLICATIONS

4.1 System Model

In this section, we will introduce the system model, body-area networks, and attack models perspectives.

4.1.1 System Overview

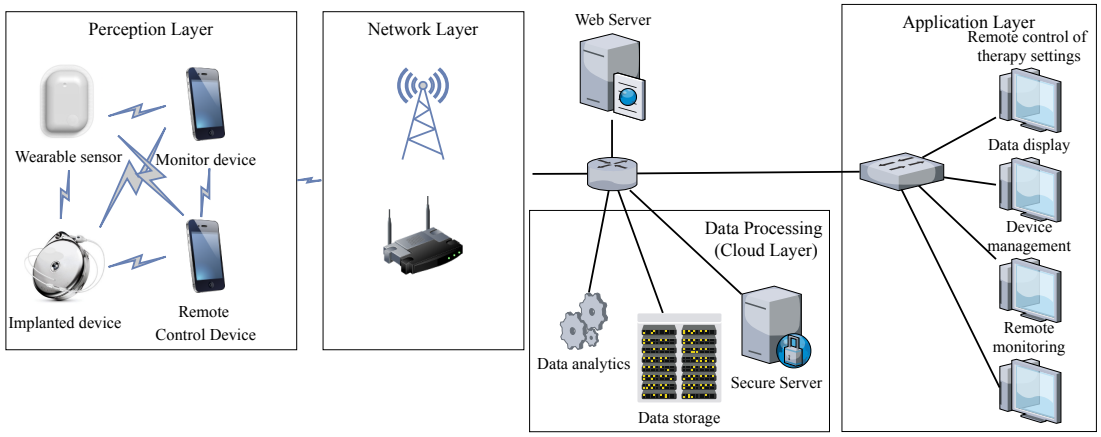

Figure 4.1: E-health overall system architecture is shown.

We consider modern medical sensing and actuation devices, including implantable devices, in our proposed system model. The medical devices maintain a wireless local network in order to monitor physiological quantities or remotely modify therapy settings. There are multiple layers to consider in the proposed system, including the perception layer, network layer, data processing layer, and application layer as shown in Fig. 4.1.

The sensors and actuators seen in the perception layer are often power-constrained, so heavyweight security is impractical. Traditionally, information has been secured at the network layer, leaving the perception layer, or in this case, the body area network vulnerable to various attacks. In Fig. 4.1, wearable sensors and implanted devices are considered. Patients' data can be collected from implanted devices and wearable sensors. Monitor devices and remote control devices can be utilized as a relay to transmit the sensed data from patients to the cloud. Security in wired communications is not considered in this thesis.

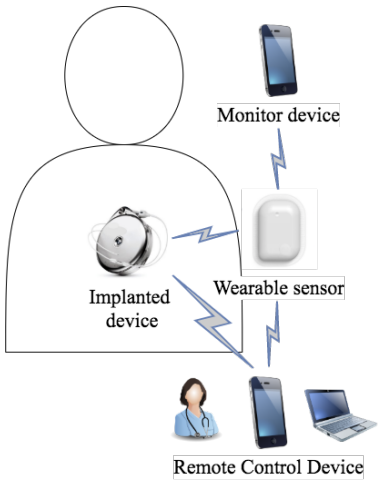

Figure 4.2: Communication between devices in the body area network of the example system.

4.1.2 The Body Area Network

For the purpose of this study, we use an insulin delivery system as an example to illustrate the types of connected medical devices present in the body area networks. For the sample system, this network will include an implanted infusion pump, a wearable blood glucose meter, a remote monitoring device, and a remote control device. Implantable insulin infusion pumps are implanted subcutaneously (under the skin), with a catheter extending from the pump into the peritoneal cavity. Implantation of insulin pumps is relatively unpopular due to the impracticality of replacement and refill, but the subcutaneous delivery of insulin is thought to more closely mimic the delivery of insulin in people without diabetes [67].

Wearable continuous blood glucose monitors take blood glucose readings regularly to provide data to monitor the user's blood sugar levels. There is a large market for continuous blood glucose monitors for patients with diabetes, and many products on the market have incorporated wireless technologies for display of data. The sensor on the continuous blood glucose monitor is a very thin wire or filament inserted with the aid of a needle under the user's skin, typically applied on the abdomen or back of the underarm. A sticky backing holds the sensor in place on the user's skin. Using similar enzymes as a test strip for a glucose meter, the sensor detects glucose in the interstitial fluid (the fluid between the cells) [68]. A wireless transmitter can attach on top of the area where the sensor was inserted to send data to a monitor device every one to five minutes. The monitor device receives data from the blood glucose meter and presents information to the user. Displays often include current glucose levels, past readings, alerts on abnormal glucose levels, status messages, and trend information. Standalone monitor devices as well as smartphone apps are available on the market. Finally, in networked medical device systems such as the one we have outlined, the capability for remote control of therapy settings by a medical professional is often incorporated into the functionality of the system. This introduces a remote control device, which has the ability to modify therapy and firmware settings on the implantable infusion pump. The wireless communication in the system is shown in Fig. 4.2.

Within the system, consideration must be given to the resource divide between devices. For example, since an implantable device may require surgery to recharge or replace a battery, it is imperative to reduce the power consumption for such a device. A smartphone application, however, may have less restrictions on power consumption and CPU usage due to the utilization of more powerful processors in most smartphones and relative ease of recharging the device.

Table 4.1: Summary of Attack Models for Networked Medical Devices

Attack Model	Implementation	Motivation of Attackers	Countermeasures	Objective of security
Eavesdropping	Universal Software Radio Peripheral	Extract sensitive exchanged data; Use compromised device to attack other sections of the healthcare network	Encryption of exchanged data; Identification and authorization of incoming traffic	Patient data privacy protection; Protection of credentials
Unauthorized Access	Universal Software Radio Peripheral; Unauthorized programmer used to capture PIN	Modify therapy settings or firmware; Drift clock; Delete stored data; Financial, nation-state, or cyber-terrorist	Tamper resistance of firmware to unauthorized reprogramming and passive secret stealing; Encryption of data stored on the device	Maintain intended device therapy settings; Preserve stored data
Denial-of-Service	Repetitive messages to the device, leading to resource depletion; Buffer overflow	Prevent device from collecting data; Prevent device from receiving configuration	Reverse DNS lookup to verify the source address	Ensure availability of the system to the desired specifications

4.1.3 Attack Models

In such a system, an attacker may have various motives, including data capture or obtaining unauthorized access to the device. Data capture can be achieved through an eavesdropping attack and the risk mitigated through the use of encryption. The risk of unauthorized access can be mitigated through the use of authentication and authorization [69]. Therefore, in our proposed system model, we consider eavesdropping, unauthorized access, and denial-of-services as shown in Table. 4.1. From Table. 4.1, we present the possible implementation of each attack model, motivation of attackers, possible countermeasures and objective of security corresponding to each attack model.

4.1.3.1 Eavesdropping

An eavesdropping attack can be performed using a Universal Software Peripheral. If messages are not encrypted, the attacker can extract sensitive exchanged data, including device identification, physiological patient data, therapy specification, and even authentication credentials exchanged in plaintext (if authentication is, in fact, used) [35]. This type of attack is targeted mainly at the network layer and can be prevented using encryption of exchanged data and identification and authorization mechanisms for incoming network traffic [34]. Again, however, encryption and authorization are costly for a power-constrained device, so many networked medical devices may omit these basic security features against an eavesdropping attack.

4.1.3.2 Unauthorized access

An unauthorized access attack can be performed using a Universal Software Peripheral or, in the case of wireless-programmable devices, even an unauthorized device programmer. Unauthorized access could allow the attacker to make modifications to therapy settings, modify the device firmware, drift the clock to make timestamps invalid or misleading, delete data stored in the device, or even disable the device altogether [69]. In order to prevent such an attack, the device firmware must be tamper-resistant to unauthorized reprogramming and passive secret stealing, and access control must be employed on each node in the system in order to prevent unauthorized access from compromising the entire system. Additionally, protection of storage should be implemented by encrypting data stored on the device using security features on the hardware [70]. However, access control and encryption are costly in terms of power consumption, so many power-constrained IoT devices (such as implantable networked medical devices) omit these critical security measures.

4.1.3.3 Denial-of-service

A denial-of-service attack is when the attacker attempts to prevent the legitimate user from accessing the networked services. This type of attack can be performed by sending repetitive messages to the device, leading to device resource depletion. Denial-of-service attacks are typically either implemented as flood attacks or buffer overflow attacks. Flood attacks send an overwhelming number of packets to a given device, saturating the target device. Buffer overflow attacks use a memory buffer overflow to cause the target device to consume all available memory or CPU time.

4.2 Case Study

In this section, we introduce a case study based on our proposed system model. We first introduce the classification of devices. Then we present different key management methods. Finally we show our test environment. Results of the experimentation are presented and discussed.

4.2.1 Device Classification

For this study, the system model outlined in Fig. 4.2 is used as a sample system. A software simulation using Python Bluetooth and AES libraries is utilized to quantify performance and energy consumption of the system for both baseline and experimental phases.

Table 4.2 outlines the basis for classification for each device in the system. From metrics such as the ease of battery recharge or replacement, it can be inferred that certain devices have greater or fewer resources practically available to implement additional functionality, such as security protocols. Additionally, the type and frequency of wireless communication

by or to a device provides information about the ease of implementing additional functionality related to the security of the wireless protocol on that device. The proposed method is to classify devices based on resource constraints, presence in the body area network, and regular wireless activity to identify certain devices to run additional wireless security protocols on in order to improve the security of the overall body area network. Using Table 4.2, the monitor device can be identified as a potential target device on which to run additional security protocols.

Table 4.2: Basis of Classification for Each Device in the System

Device	Time to replacement or battery recharge	Availability in the body network	Primary function	Wireless communication
Implanted infusion pump	4 - 7 years (replacement)	Always	Drug delivery	Receiver
Wearable sensor	7 - 14 days (replacement)	Always (except during replacement)	Obtaining physiologic data	Sends data every 1 - 5 minutes
Monitor device	12 - 24 hours (recharge)	Usually	Data presentation	Receiver
Remote control device	12 - 24 hours (recharge)	Occasionally	Changing therapy settings on implantable device	Sends data as necessary

The monitor device is often a smartphone application, thus lending the resources of the relatively powerful smartphone hardware. Most smartphone users charge their device regularly and consistently keep it in range of the body area network. Furthermore, the monitor device is often receiving communications from other devices in the network about the user's physiological data. Since security can be a heavy consumer of a device's power and CPU resources, it is important to consider these metrics in device categorization. Furthermore, consistent presence of the device in the network and consistent wireless communication between this device and other devices in the network are important for availability to search for active threats. For these reasons, the user's smartphone is a good candidate to implement additional security-related functionality in the body area network.

Based on power and CPU constraints on each device in the system, the devices can be classified into three primary categories:

1. Level 1: Implanted device;
2. Level 2: Wearable device;
3. Level 3: Smartphone (monitor device or remote control device).

In this device classification scheme, the implanted device is considered to be the most energy and hardware constrained due to the impracticality of recharge or replacement, while the smartphone is considered the least energy constrained due to ease of recharge and relatively powerful processor.

4.2.2 Key Management Methods

There are three different key management methods considered in this thesis: a baseline method using homogeneous key management, semi-heterogeneous key management and heterogeneous key management.

4.2.2.1 Baseline Method: Homogeneous Key Management

In this baseline method, each class of device implements the same symmetric key generation, distribution, and management techniques as shown in Fig. 4.3. This is simulated by each device performing a key refresh for one link in the system by hashing the old symmetric encryption key for that link and distributing this key using the old encryption key. The receiving device for this link in the system decrypts the new key using the old encryption key and installs the new key.

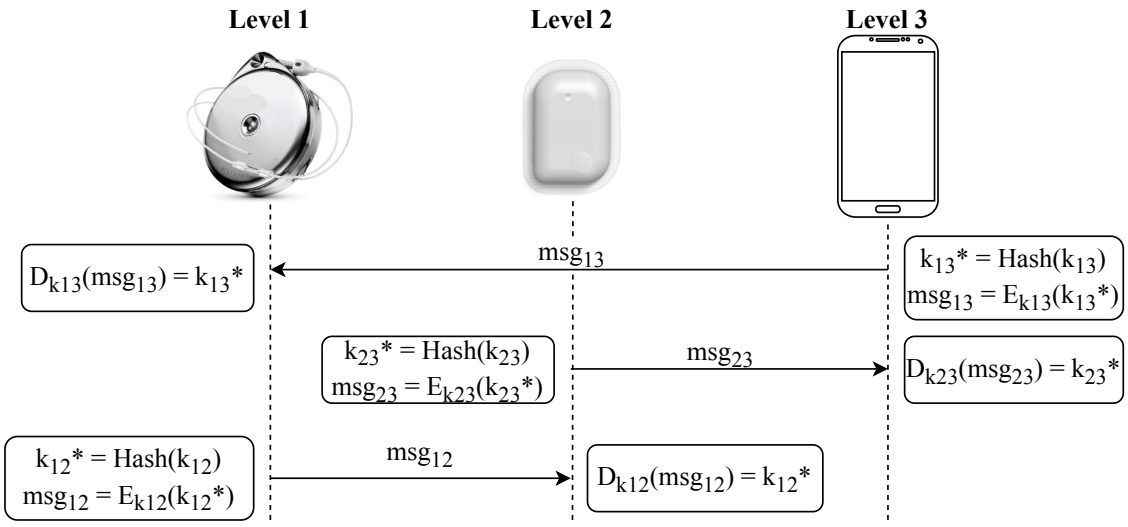

Figure 4.3: The baseline key management scheme with a homogeneous system model is shown.

4.2.2.2 Semi-heterogeneous Key Management

We propose a system in which key management is handled in an asymmetric manner between devices, depending on the energy restraints of the device. In this method, the Level 3 device (smartphone) is utilized to implement symmetric key generation, distribution, and management for links with the Level 1 (implanted) and Level 2 (wearable) devices in the system. Furthermore, the Level 3 device performs session key generation, distribution, and refresh functionality to the Level 1 - Level 2 link using its previously established connections with both the Level 1 and Level 2 devices. The new key is generated based on a hash of the old symmetric encryption key and distributed by encrypting the new key using the old encryption key. When the second device receives the encrypted key, it decrypts the message with the old key and installs the new key. This key management scheme is shown in Fig. 4.4.

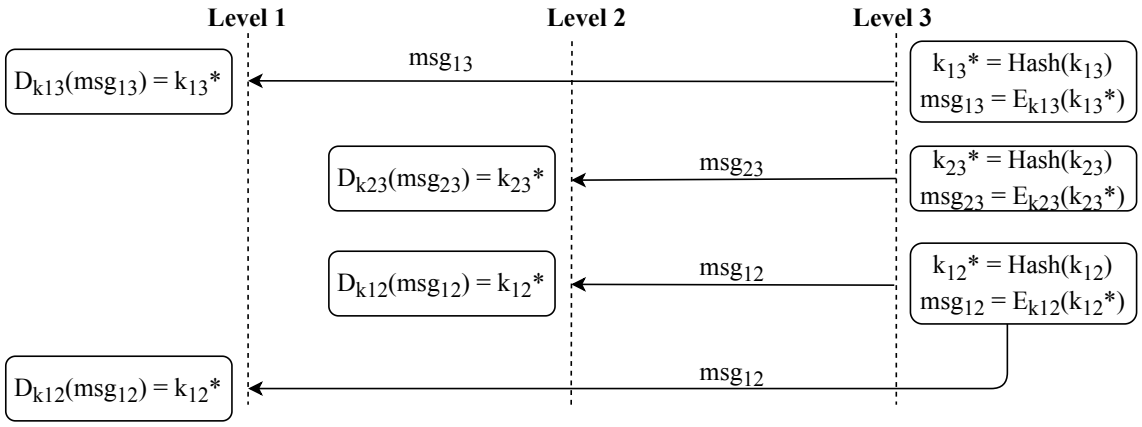

Figure 4.4: A semi-heterogeneous key management scheme is shown which differentiates between Level 3 (smartphone) devices and other devices in the system.

4.2.2.3 Heterogeneous Key Management

In the second experimental method, a similar method to the previous experimental method is used, except the symmetric encryption key used to secure links with the Level 1 (implanted) device are generated using PUF-based key generation [71]. PUFs (or Physical Unclonable Functions) use entropy created by variations within tolerances of manufacturing processes of electronics to produce a function that is unique to a particular device. When a PUF is used to hash a random number, this can be an effective low-power method of performing key generation. PUFs, which have become a popular hardware security approach in recent years, can be found on embedded systems, but are rarely included in higher-power computing applications such as smartphones. For this reason, we make the assumption that a PUF is present in the Level 1 (least-resourced) device in the system.

In this method, instead of receiving the new key encrypted by the old key, the implanted device hashes a random number generated by the Level 3 device in order to generate a new encryption key. The Level 3 device performs the same hash with the same random number in order to generate the key for the other device in the link. For the Level 1 - Level 2 link in the system, the Level 3 device performs this hash of the random number and distributes

it to the Level 2 device using the encryption key for the pre-established Level 2 - Level 3 link. This key management protocol is shown in Fig. 4.5.

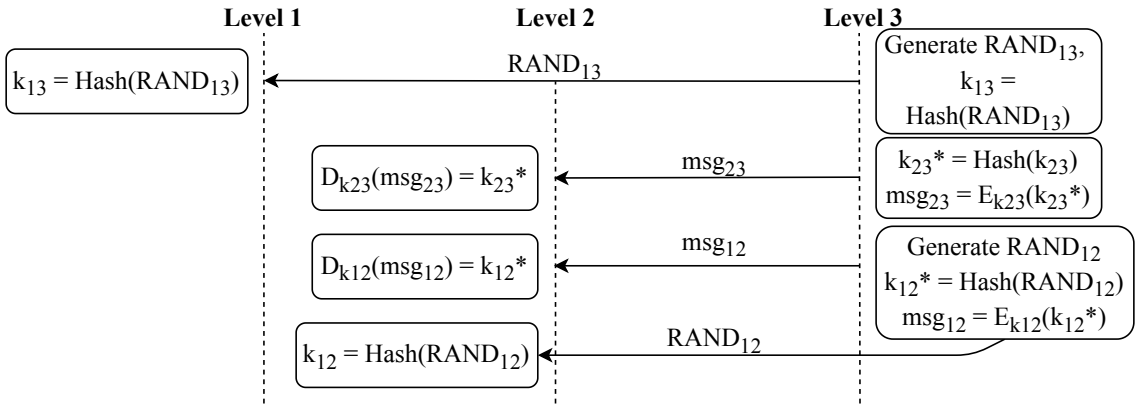

Figure 4.5: A heterogeneous key management scheme is shown which utilizes PUF-based key generation methods for the implanted device.

4.2.3 Test Environment

The following protocols and algorithms were utilized in this case study:

1. Bluetooth LE (BLE) version 4.0 with Just Works pairing and Level 1 security
2. AES encryption and decryption with 128-bit keys
3. SHA2 (Secure Hash Algorithm 2) with a 256-bit digest
4. Random number generation

Python libraries supporting Bluetooth LE (BLE), AES encryption and decryption, random number generation, and cryptographic hash functions were utilized to create a software simulation of both the baseline and experimental methods. The Adafruit Python Bluefruit LE library [72] was used for BLE support to transmit and receive all messages. This library requires an environment running Mac OSX (used in this experiment) or Linux with

a Bluetooth 4.0 low energy adapter. For two-way communication, a virtual peripheral was created on the iPhone LightBlue® application [73], using Bluetooth 4.0 low energy. In virtual peripheral mode, in the LightBlue® application, the iOS device advertises as that particular BLE peripheral. LightBlue® allows customization of the services and characteristics of any virtual peripheral, a service with read and write properties was created for this experiment to interface with the program running on the Mac OSX laptop. The PyCrypto library [74] was used for AES support, including AES encryption and decryption with 128-bit keys. Security is quantified based on symmetric encryption key size, where a 128-bit cryptographic key is more secure than a 64-bit key. The Hashlib library [75] SHA256 function was used for cryptographic hash functions. The SHA256 function utilizes SHA2 (Secure Hash Algorithm 2) with a digest of 256 bits in order to produce cryptographically secure hashes. Finally, the Python OS library was used for random number generation [76]. We recognize that using Python's built-in OS library to generate random numbers could be potentially misleading since this is simulating processes that would be run on embedded systems in the real-world, most likely in a low-level language like C. However, since many Python routines utilize C functions for performance, we assert here that using a standard Python library for random number generation is a reasonable assumption.

Performance results were produced for each of the following processes within each experimental method: 1) BLE transmission, 2) BLE receipt, 3) AES encryption, 4) AES decryption, 5) Random number generation, 6) SHA2 256-bit hash.

The appropriate timing results were added for each experimental method for each device class, and the results were plotted by device class. A sample size of a thousand timing results for each process was used for this experiment.

4.2.4 Results

Execution times for each process (BLE transmission, BLE receipt, AES encryption, AES decryption, random number generation, and SHA2 256-bit hash) are shown in Fig. 4.6.

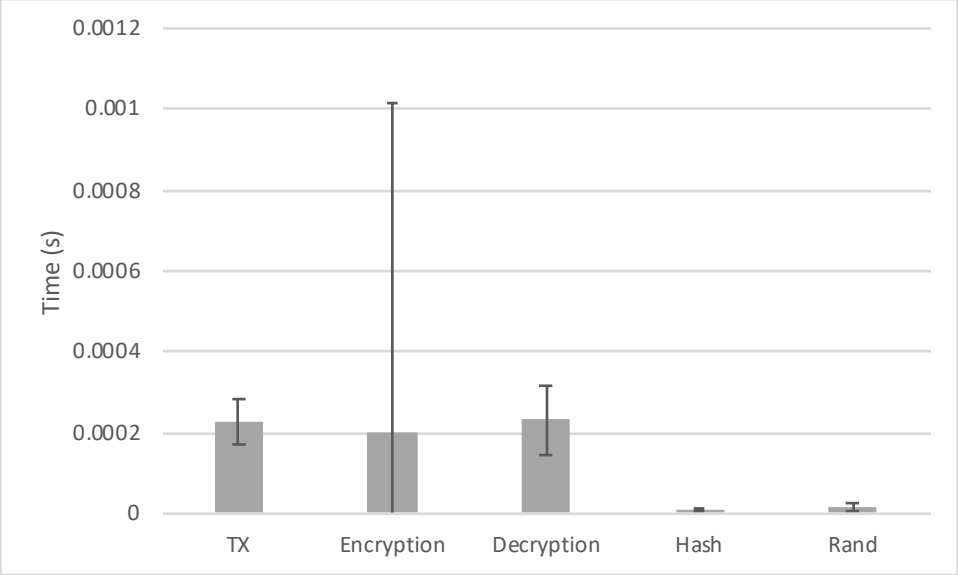

Figure 4.6: The breakdown of execution times by process is shown, with error bars to +/- one standard deviation.

The time used for key management for each method described previously is plotted by device classification level, as shown in Fig. 4.7 and Fig. 4.8. In Fig. 4.7 the normalized key management time is shown on the y-axis, for each experimental method described in Section 4.2.2 (x-axis). Fig. 4.8 shows the absolute execution time (y-axis) for each device and key management method (x-axis).

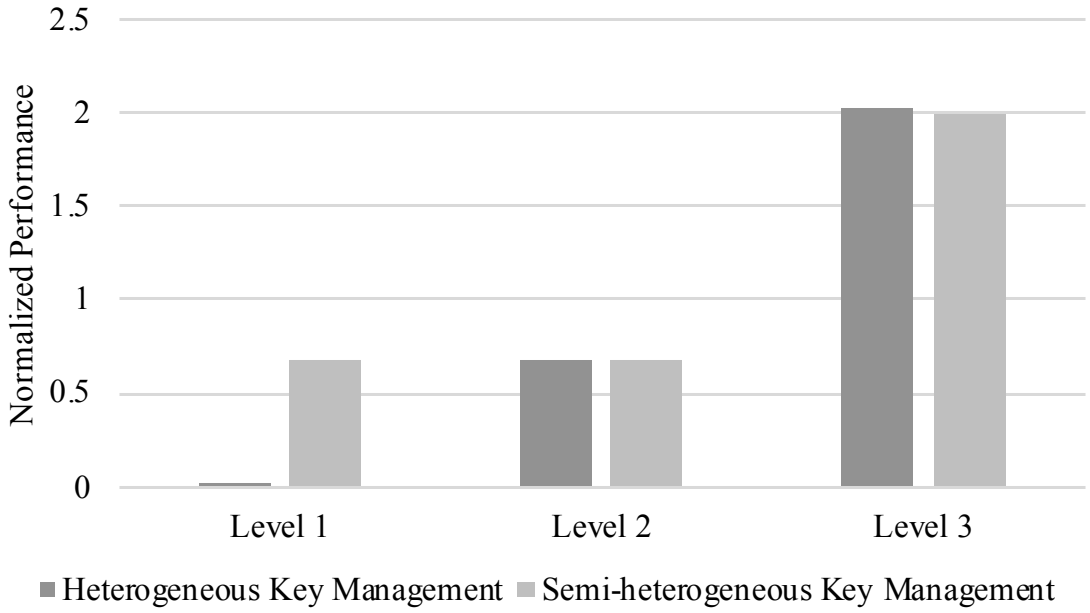

Figure 4.7: Normalized key management time for each experimental method is presented as a fraction of key management time using the baseline (homogeneous) method, for each classification level of device in the system.

For the baseline method, Fig. 4.8 shows that the time used for key management by device is the same for the homogeneous system model. For the semi-heterogeneous system model, we see that the asymmetric key management method, which exploits the heterogeneous devices, results in less time being used by the Level 1 and Level 2 devices, which is instead incurred by the Level 3 device, as the Level 3 device assumes additional key management responsibilities. In this method, the key management time for the Level 1 and Level 2 devices is the same. For the heterogeneous system model involving PUF-based key generation for the implanted device, it can be seen that the key management time for the Level 1 (implanted device) is further reduced (in fact the performance overhead nearly negligible for the Level 1 device). This is primarily due to the fact that a hash of a random number as utilized in the PUF-based method is less costly than decryption, as were seen in the previous methods.

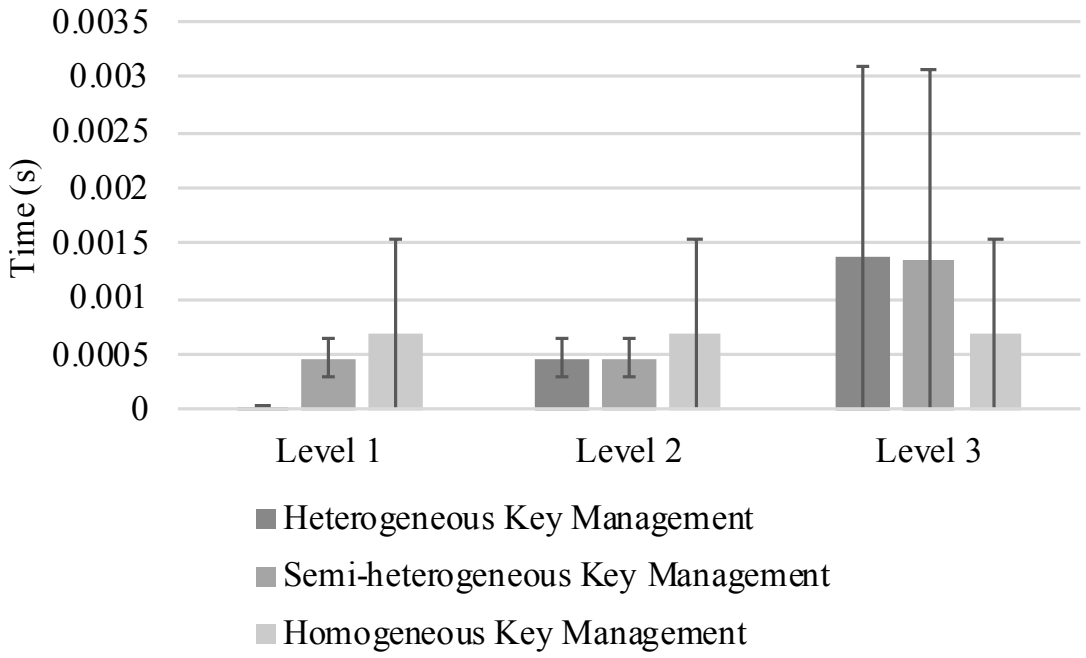

Figure 4.8: The time used for key management activities is shown by device for each of three system models: the baseline, a homogeneous system model, a semi-heterogeneous system model, and a heterogeneous system model in which the implanted device utilizes PUF-based key generation methods. Error bars are shown for one standard deviation.

A two-sample, two-tailed t-test assuming unequal variance was used to determine whether the timing results differed significantly for each experimental method from the baseline method, for each device classification level. A significance level of 0.05 was used to determine significance with a 95% confidence level. Table 4.3 displays p-values and corresponding significance results for each device classification level in each experimental method. These results demonstrate that the time used in key management is significantly reduced from the baseline for both of the experimental methods (heterogeneous and semi-heterogeneous), for all classes of devices - Level 1, Level 2, and Level 3.

Table 4.3: T-test Results (P-Values) Comparing Experimental Methods to Baseline

Experimental Method	Level 1	Level 2	Level 3
Semi-heterogeneous Key Management	1.99E-14	1.99E-14	1.99E-27
Heterogeneous Key Management with PUF	9.18E-104	1.99E-14	6.36E-29

4.3 Conclusions: Heterogeneous System Model for E-health

In this section, we first proposed a system model with consideration of the limitations of each device in an e-health body area network. We then proposed a classification system to separate devices into different levels based on the constraints of the specific device. Finally, we provided a case study utilizing the device classifications to implement a heterogeneous security system which results in less resource depletion for resource-limited devices. The case study has applied semi-heterogeneous and heterogeneous experimental methods which address key management. Results from the case study show that it is possible to significantly reduce the time used for key management activities on power-constrained devices by utilizing semi-heterogeneous and heterogeneous system models as a basis for the distribution of security responsibilities.

The case study uses key management as an example of a security application which can be asymmetrically distributed across devices in the system; however, there is potential to expand this idea to other security or privacy protocols in such a system. For example, anomaly detection software could be run on less resource-constrained devices in the system in order to provide a threat detection mechanism for additional security. Additionally, the timing results in this case study were performed as a Python software simulation, so it would be interesting to see the results on hardware with realistic specifications to the application given, in order to measure power consumption for each method in a more realistic setting.

Chapter 5

CONCLUSIONS

E-health is transforming the field of healthcare in an effort to provide effective, efficient access to healthcare and perform remote patient monitoring for early detection and treatment of health conditions. E-health systems are made possible by the introduction of networked medical devices, which form a body area network along with a gateway device (often the user's smartphone). As such systems become more prevalent, it is important to think about the implications and practicality of securing these systems. Patient data privacy, data integrity, and availability of devices in the system are three important considerations in e-health wireless security. As medical devices become increasingly network-connected with the development of remote patient monitoring and the Internet of Things, e-health applications have been developing rapidly. Privacy of patient information and security of critical device firmware settings are a significant concern; however, with power and computational resources of many of these embedded systems, implementing traditional network security measures is impractical.

In the first two sections of this thesis, we survey current approaches to e-health security and privacy, providing a general e-health system model, outlining challenges and threats, providing security and privacy objectives, and surveying and classifying current solutions. Our survey suggests the potential for further study in e-health security and privacy, given that e-health is a relatively new field and many e-health systems in industry operate without effective security and privacy threat mitigations in place. In the final section of this thesis, we first proposed a system model with consideration of the limitations of each device in an e-health body area network. We then proposed a classification system to separate devices into different levels based on the constraints of the specific device. Finally, we provided a

case study utilizing the device classifications to implement a heterogeneous security system which results in less resource depletion for resource-limited devices.

There is a lot of work still be done to address wireless security and privacy concerns in the field of e-health, especially due to the sensitive nature of the data being transmitted and the unique constraints of medical devices. E-health promises a way to increase access to healthcare and has been steadily growing in popularity, so it is important to secure this platform as we move into the future.

BIBLIOGRAPHY

[1] Laurinda B Harman, Cathy A Flite, and Kesa Bond. Electronic health records: privacy, confidentiality, and security. *AMA Journal of Ethics*, 14(9):712–719, 2012.

[2] El Khaddar, Mehdia Ajana, Hamid Harroud, Mohammed Boulmalf, Mohammed Elkoutbi, and Ahmed Habban. Emerging wireless technologies in e-health trends, challenges, and framework design issues. *2012 International Conference on Multimedia Computing and Systems, IEEE*, pages 440–445, 2012.

[3] Olga Boric-Lubecke, Xiaomeng Gao, Ehsan Yavari, Mehran Baboli, Aditya Singh, and Victor M Lubecke. E-healthcare: Remote monitoring, privacy, and security. In *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*, pages 1–3. IEEE, 2014.

[4] Hamid Sharif, Michael Hempel, Thomas Mikchael Bohnert, and Ali Khoynezhad. Wireless communications for e-health applications [guest editorial]. *IEEE Wireless Communications*, 20(4):10–11, 2013.

[5] Harsha S Gardiyawasam Pussewalage and Vladimir A Oleshchuk. Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions. *International Journal of Information Management*, 36(6):1161–1173, 2016.

[6] Sherali Zeadally, Jesús Téllez Isaac, and Zubair Baig. Security attacks and solutions in electronic health (e-health) systems. *Journal of medical systems*, 40(12):263, 2016.

[7] Rajendra Kumar Dwivedi, Sonali Pandey, and Rakesh Kumar. A study on machine learning approaches for outlier detection in wireless sensor network. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pages 189–192. IEEE, 2018.

[8] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh. Secured data collection with hardware-based ciphers for iot-based healthcare. *IEEE Internet of Things Journal*, 6(1):410–420, 2019.

[9] Barbara L Filkins, Ju Young Kim, Bruce Roberts, Winston Armstrong, Mark A Miller, Michael L Hultner, Anthony P Castillo, Jean-Christophe Ducom, Eric J Topol, and Steven R Steinhubl. Privacy and security in the era of digital health: what should translational researchers know and do about it? *American journal of translational research*, 8(3):1560, 2016.

[10] Ramon Martí, Jaime Delgado, and Xavier Perramon. Security specification and implementation for mobile e-health services. In *IEEE International Conference on e-Technology, e-Commerce and e-Service, 2004. EEE'04. 2004*, pages 241–248. IEEE, 2004.

[11] US Department of Health, Human Services, et al. Modifications to the hipaa privacy, security, enforcement, and breach notification rules under the health information technology for economic and clinical health act and the genetic information nondiscrimination act; other modifications to the hipaa rules. *Federal register*, 78(17):5566–5702, 2013.

[12] World Health Organization et al. Legal frameworks for ehealth: Based on the findings of the second global survey on ehealth. global observatory for ehealth series. geneva: Who; 2012.

[13] Tony Sahama, Leonie Simpson, and Bill Lane. Security and privacy in ehealth: Is it possible? In *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, pages 249–253. IEEE, 2013.

[14] Nureni Ayofe Azeez and Charles Van der Vyver. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal*, 20(2):97–108, 2019.

[15] José Luis Fernández-Alemán, Inmaculada Carrión Señor, Pedro Ángel Oliver Lozoya, and Ambrosio Toval. Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3):541–562, 2013.

[16] Shekha Chenthara, Khandakar Ahmed, Hua Wang, and Frank Whittaker. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, 7:74361–74382, 2019.

[17] Assad Abbas and Samee U Khan. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics*, 18(4):1431–1441, 2014.

[18] Achraf Ben Amar, Ammar B Kouki, and Hung Cao. Power approaches for implantable medical devices. *sensors*, 15(11):28889–28914, 2015.

[19] Patricia AH Williams and Andrew J Woodward. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices (Auckland, NZ)*, 8:305, 2015.

[20] Dongfeng Fang and Feng Ye. Identity management framework for e-health systems over 5g networks. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[21] Virtuoso dr/vr d154awg/ d154vwc reference manual, 2019.

[22] US Food, Drug Administration, et al. Cybersecurity vulnerabilities affecting medtronic implantable cardiac devices, programmers, and home monitors: Fda safety communication, 2019.

[23] Heena Rathore, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, and Mohsen Guizani. A review of security challenges, attacks and resolutions for wireless medical devices. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1495–1501. IEEE, 2017.

[24] Tehreem Yaqoob, Haider Abbas, and Mohammed Atiquzzaman. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. *IEEE Communications Surveys & Tutorials*, 21(4):3723–3768, 2019.

[25] Nourhene Ellouze, Mohamed Allouche, Habib Ben Ahmed, Slim Rekhis, and Noureddine Boudriga. Security of implantable medical devices: limits, requirements, and proposals. *Security and Communication Networks*, 7(12):2475–2491, 2014.

[26] Jungchae Kim, Byuck jin Lee, and Sun K Yoo. Design of real-time encryption module for secure data protection of wearable healthcare devices. In *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 2283–2286. IEEE, 2013.

[27] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. A flexible and efficient authentication and secure data transmission scheme for iot applications. *IEEE Internet of Things Journal*, 7(4):3474–3484, 2020.

[28] Tamara Denning, Kevin Fu, and Tadayoshi Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *HotSec*, 2008.

[29] Fengyuan Xu, Zhengrui Qin, Chiu C Tan, Baosheng Wang, and Qun Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *2011 Proceedings IEEE INFOCOM*, pages 1862–1870. IEEE, 2011.

[30] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. In *Proceedings of the ACM SIGCOMM 2011 conference*, pages 2–13, 2011.

[31] Ahmed Alahmadi and Ben Soh. A smart approach towards a mobile e-health monitoring system architecture. In *2011 International Conference on Research and Innovation in Information Systems*, pages 1–5. IEEE, 2011.

[32] Heena Rathore, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, and Mohsen Guizani. A review of security challenges, attacks and resolutions for wireless medical devices. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1495–1501. IEEE, 2017.

[33] Tehreem Yaqoob, Haider Abbas, and Mohammed Atiquzzaman. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. *IEEE Communications Surveys & Tutorials*, 21(4):3723–3768, 2019.

[34] Ahmad W Atamli and Andrew Martin. Threat-based security analysis for the internet of things. In *2014 International Workshop on Secure Internet of Things*, pages 35–43. IEEE, 2014.

[35] Nourhene Ellouze, Mohamed Allouche, Habib Ben Ahmed, Slim Rekhis, and Noureddine Boudriga. Security of implantable medical devices: limits, requirements, and proposals. *Security and Communication Networks*, 7(12):2475–2491, 2014.

[36] Duygu Karaoğlan Altop, Albert Levi, and Volkan Tuzcu. Deriving cryptographic keys from physiological signals. *Pervasive and Mobile Computing*, 39:65–79, 2017.

[37] Daniel Halperin, Thomas S Heydt-Benjamin, Benjamin Ransford, Shane S Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 129–142. IEEE, 2008.

[38] Byungjo Kim, Jiung Yu, and Hyogon Kim. In-vivo nfc: Remote monitoring of implanted medical devices with improved privacy. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, pages 327–328, 2012.

[39] Sarbari Gupta. Implantable medical devices-cyber risks and mitigation approaches. In *Proceedings of the Cybersecurity in Cyber-Physical Workshop, The National Institute of Standards and Technology (NIST), US*, 2012.

[40] Xiali Hei, Xiaojiang Du, Jie Wu, and Fei Hu. Defending resource depletion attacks on implantable medical devices. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–5. IEEE, 2010.

[41] Jungchae Kim, Byuck jin Lee, and Sun K Yoo. Design of real-time encryption module for secure data protection of wearable healthcare devices. In *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 2283–2286. IEEE, 2013.

[42] MJM Chowdhury, ASM Kayes, Paul Watters, Patrick Scolyer-Gray, and Alex Ng. Patient controlled, privacy preserving iot healthcare data sharing framework. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[43] Entao Luo, Md Zakirul Alam Bhuiyan, Guojun Wang, Md Arafatur Rahman, Jie Wu, and Mohammed Atiquzzaman. Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems. *IEEE Communications Magazine*, 56(2):163–168, 2018.

[44] Keyur Tapan Shah. *Privacy and Security Issues of Wearables in Healthcare*. PhD thesis, Flinders University, College of Science and Engineering., 2019.

[45] Christian Esposito, Alfredo De Santis, Genny Tortora, Henry Chang, and Kim-Kwang Raymond Choo. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 5(1):31–37, 2018.

[46] Farzana Rahman, Md Zakirul Alam Bhuiyan, and Sheikh Iqbal Ahamed. A privacy preserving framework for rfid based healthcare systems. *Future Generation Computer Systems*, 72:339–352, 2017.

[47] M. Z. A. Bhuiyan, M. Zaman, G. Wang, T. Wang, and J. Wu. Privacy-protected data collection in wireless medical sensor networks. In *2017 International Conference on Networking, Architecture, and Storage (NAS)*, pages 1–2, 2017.

[48] Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M Shamim Hossain, Ahmad Almogren, and Atif Alamri. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access*, 5:22313–22328, 2017.

[49] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. Medibchain: A blockchain based privacy preserving platform for

healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage*, pages 534–543. Springer, 2017.

[50] Yang Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, and Victor Chang. Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system. *Information Sciences*, 479:567–592, 2019.

[51] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, 95:511–521, 2019.

[52] Liviu Hirtan, Piotr Krawiec, Ciprian Dobre, and Jordi Mongay Batalla. Blockchain-based approach for e-health data access management with privacy protection. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–7. IEEE, 2019.

[53] Yan Li, Changxin Bai, and Chandan K Reddy. A distributed ensemble approach for mining healthcare data under privacy constraints. *Information sciences*, 330:245–259, 2016.

[54] Jingjing Wang, Xiaoyu Zhang, Jingjing Guo, and Jianfeng Wang. Security analysis of" pslp: Privacy-preserving single-layer perceptron learning for e-healthcare". *IACR Cryptology ePrint Archive*, 2017:405, 2017.

[55] Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, 40(10):218, 2016.

[56] Sagar Sharma, Keke Chen, and Amit Sheth. Toward practical privacy-preserving analytics for iot and cloud-based healthcare systems. *IEEE Internet Computing*, 22(2):42–51, 2018.

[57] Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu, and Danyi Li. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–5. IEEE, 2017.

[58] Abdul Majeed. Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data. *Journal of King Saud University-Computer and Information Sciences*, 31(4):426–435, 2019.

[59] Usama Salama, Lina Yao, Xianzhi Wang, Hye-young Paik, and Amin Beheshti. Multi-level privacy-preserving access control as a service for personal healthcare monitoring. In *2017 IEEE International Conference on Web Services (ICWS)*, pages 878–881. IEEE, 2017.

[60] Oluwabiyi Akinkunmi, Muhammad Ehsan Rana, et al. Privacy preserving data publishing anonymization methods for limiting malicious attacks in healthcare records. *Journal of Computational and Theoretical Nanoscience*, 16(8):3538–3543, 2019.

[61] S Sneha and P Asha. Privacy preserving on e-health records based on anonymization technique. *Global Journal of Pure and Applied Mathematics*, 13(7):3367–3380, 2017.

[62] Ari Juels. Privacy-protecting system and method for wireless medical devices, March 12 2019. US Patent 10,230,699.

[63] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[64] George Robert Blakley. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318. IEEE, 1979.

[65] Andrea Damiani, Carlotta Masciocchi, Luca Boldrini, Roberto Gatta, Nicola Dinapoli, Jacopo Lenkowicz, Giuditta Chiloiro, Maria Gambacorta, Luca Tagliaferri, Rosa Autorino, et al. Preliminary data analysis in healthcare multicentric data mining: a privacy-preserving distributed approach. *Journal of E-learning and Knowledge Society*, 14(1), 2018.

[66] Marios Vardalachakis, Haridimos Kondylakis, Lefteris Koumakis, Angelina Kouroubali, and Dimitrios G Katehakis. Shinyanonymizer: A tool for anonymizing health data. In *International Conference on Information and Communication Technologies for Ageing Well and e-Health, ICT4AWE*, 2019.

[67] Nienke A Spaan, Alina E Teplova, Eric Renard, and Jos AE Spaan. Implantable insulin pumps: an effective option with restricted dissemination. *The Lancet Diabetes & Endocrinology*, 2(5):358–360, 2014.

[68] Continuous glucose monitoring, 2017.

[69] Nourhene Ellouze, Mohamed Allouche, Habib Ben Ahmed, Slim Rekhis, and Noureddine Boudriga. Security of implantable medical devices: limits, requirements, and proposals. *Security and Communication Networks*, 7(12):2475–2491, 2014.

[70] Ahmad W Atamli and Andrew Martin. Threat-based security analysis for the internet of things. In *2014 International Workshop on Secure Internet of Things*, pages 35–43. IEEE, 2014.

[71] G Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference*, pages 9–14. IEEE, 2007.

[72] Bluefruit le. `https://github.com/adafruit/Adafruit_Python_BluefruitLE`.

[73] Lightblue app. `https://apps.apple.com/us/app/lightblue/id557428110`.

[74] Pycrypto. `https://github.com/dlitz/pycrypto`.

[75] Hashlib. `https://docs.python.org/3/library/hashlib.html`.

[76] Python os. `https://docs.python.org/3/library/os.html`.