Attacks and Countermeasures in IoT Based Smart Healthcare Applications

Haque A.K.M. Bahalul, Bhushan Bharat, Nawar Afra, Talha Khalid Raihan, Ayesha Sadia Jeesan

DOI: 10.1007/978-3-030-90119-6_6

Attacks and Countermeasures in IoT based Smart Healthcare Applications

AKM Bahalul Haque,
LUT School of Engineering Sceince, LUT University, Finland.
Email- bahalul.haque@lut.fi

Bharat Bhushan,
Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, India.
Email- bharat_bhushan1989@yahoo.com

Afra Nawar,
Dept. of Electrical and Computer Engineering, North South University, Bangladesh.
Email: afra.nawar05@northsouth.edu

Khalid Raihan Talha,
Dept. of Electrical and Computer Engineering, North South University, Bangladesh.
Email: khalid.talha@northsouth.edu

Sadia Jeesan Ayesha,
Dept. of Electrical and Computer Engineering, North South University, Bangladesh.
Email: sadia.ayesha@northsouth.edu

Abstract

The perpetual evolution of IoT continues to make cities smart beyond measure with the abundance of data transactions through expansive networks. Healthcare has been a foremost pillar of settlements and has gained particular focus in recent times owing to the pandemic and the deficiencies it has brought to light. There is an exigency to developing smart healthcare systems that make smart cities more intelligent and sustainable. Therefore, this paper aims to present a study of smart healthcare in the context of a smart city, along with recent and relevant research areas and applications. Several applications have been discussed for early disease diagnosis and emergency services with advanced health technologies. It also focuses on security and privacy issues and the challenges posed by technologies such as wearable devices and big healthcare data. This paper briefly reviews some enhanced schemes and recently proposed security mechanisms as countermeasures to various cyber-attacks. Recent references are primarily used to present smart healthcare privacy and security issues. The issues are laid out briefly based on the different architecture layers, various security attacks, and their corresponding proposed solutions along with other facets of smart health such as Wireless Body Area Network (WBAN) and healthcare data.

Keywords: Smart Healthcare, Smart City, IoT, Security, Privacy

9.1. Introduction

In this modern era, the population of urban areas is increasing rapidly. So, the needs of the citizens are also increasing. The conventional supply management is not sufficient enough to support the requirements of the urban area and citizens. Smart cities play a vital role in ensuring maximum comfort to the citizens. The concept uses information and communication technology (ICT) to fulfill all the necessary functional and environmental requirements of an urban area [1]. In other words, ICT and urban functions get integrated or combined. In a broad sense, smart cities are a combination of ICT technologies, ecological environment, energy management technologies, and supportive families within the urban and rural areas [2], [3].

The idea of a smart city was introduced due to some particular reasons. One of the reasons is that a significant number of jobs is taking place in urban areas. The majority of the citizens move to urban areas by making it denser than before [4]. Another reason is to ensure an excellent educational opportunity for their children; many families are moving to urban areas from rural areas [5]. Many problems occur in the case of facilities and urban areas' environment to cope with this expansion. The idea of the smart city comes to play a vital role in eliminating these types of problems. It is essential to employ smart cities' necessary infrastructure, various sensors, and supportive technologies in urban areas. The Internet of Things (IoT) is said to be one of the essential concepts that can be implemented successfully in a smart city [6]. A vast commercial objective of IoT is driven by the extraordinary growth of digital devices such as sensors, actuators, smartphones, and smart gears etc [7].

There has been a fair amount of research that focuses on smart healthcare systems. Emergency healthcare is now creating possibilities from recent studies [8]. Remote healthcare monitoring can be used to monitor the physical condition of non-critical patients at home to reduce the workload on the hospitals. It is now possible to monitor the patient using wearable sensors and vision-based technologies (cameras) around the home to observe behavior patterns, tremors, and general activity levels [9]. In the future, machine learning can be introduced to have a more accurate system. Nowadays, a practical system has been developed to measure blood glucose level where patients have to give blood samples manually [10]. Heart attack can be detected by the utilization of ready-made components with built-in antennas [11].

Since smart healthcare deals with sensitive personal data, it needs to be secured properly. Data breach in healthcare sectors can be catastrophic. Patients personal will be out in the open and those can be used for identity theft, blackmail and many other reasons. IoT infrastructures can face various types of attacks which needs to be thoroughly studied, so that smart healthcare sector can be more resilient and provide integrity of services.

This paper comprises a brief introduction to the smart city architecture and an extensive analysis of attacks and countermeasures on smart healthcare infrastructure. In addition to this, a tabular representation of the recent work done on healthcare applications has been presented, which further enhances this paper's novelty. A summary of the contribution of this work has been listed below:

- An overview of a smart city, including that of its layers and fundamental pillars

- An elaborate discussion on smart healthcare in an IoT based smart city.
- Categorized discussion of smart healthcare applications alongside tabularized recent applications.
- Frequently occurring cyber-attacks in the healthcare domain and their existing security measures.
- Challenges and future research opportunities of Smart Healthcare.

The rest of this research, excluding the introduction, has been categorized into five different sections where section 2 focuses on the smart city fundamentals, its layers, and its pillars. In section 3, a broad description of smart healthcare and its vital characteristics have been included. Section 4 discusses the issues and vulnerabilities associated with the healthcare sector and also their proposed countermeasures. Section 5 emphasizes the challenges and future research directions. Finally, section 6 concludes the presented work.

9.2. Smart City Fundamentals

Although the descriptions fall on a broad spectrum when defining the concept of smart cities, they are generally acknowledged to be extensively interconnected settlements which modern cities are inevitably shaping into. A smart city "tracks and integrates conditions of its critical infrastructure" [12] and is characterized by IBM as one that is intelligent, interconnected, and instrumented [13]. Smart cities provide upgraded services to citizens by seeking and distinguishing intelligent solutions and creating thriving cities of the future [14]. They must make "conscious decisions to aggressively deploy technology as a catalyst to solving its social and business needs" [15]. Smart cities allow decision-makers to base their decisions on comprehensive and relevant data sources and improve every city aspect's efficiency. The IoT network collect data while communicate with each other. As the population density in urban areas faces unprecedented growth [16], the need for this interconnection through technology has become essential. Connectivity through the internet serves as a fundamental block in the smart city architecture. Digital devices are employed in various services that rely on it to communicate with other devices [17,18].

9.2.1 Smart City Layers

The development of the internet leads to better interconnection and an enhancement in a smart city's infrastructure. Strictly, the technical architecture of a smart city is implemented by several layers. Brief description of those layers are given below-

9.2.1.1 Sensing Layer

This layer works for data acquisition. The methods and equipment utilized in data acquisition are dependent upon the nature of the data and context. The sizable extent of smart city operations creates substantial variegated data and introduces considerable complexity in implementing the sensing layer [19]. Networks of responsive and self-regulating physical devices are employed in data collection[20]. This network of nodes captures various forms of data and environment variables like temperature, humidity, pressure, etc. which can necessitate the use of multi-featured nodes equipped with temperature sensors, cameras, GPS, and other equipment. The extent of the network in this layer has been linked to the smart city [21].

9.2.1.2 Network Layer

This layer facilitates the transmission of collected data from the sensing equipment to processing stations. Satellite, wireless, and wired communications enable transmissions within sensing networks and processing stations. Existing and developing technologies like Bluetooth, radio frequency identification (RFID), Wi-Fi, 3G, 4G, 5G, LP-WAN, and others are employed for this task.

9.2.1.3 Analysis Layer

The processing, analysis, manipulation, organization, and storage of the raw data is handled in the Analysis Layer. The processing and other tasks can be carried out on smartphones and similar terminal devices. However, a more sizable amount of data may require the usage of cloud computing platforms. Cloud computing platforms for the network layer are applicable particularly for sensor networks that generate a large quantity of data [22].

9.2.1.4 Application Layer

This layer includes the services which utilize the IoT-generated data, processed for specialized applications in various domains such as healthcare, mobility, surveillance etc. Most recently collected data and historical data generated in the equivalent context can provide the basis for quick service to various phenomena through applications using decision-making algorithms.

9.2.2 Pillars of Smart City

Smart cities are also characterized by fundamental pillars that constitute smart infrastructure, smart society and public, smart environment, and smart governance and management, which can be further subdivided into multiple areas of concern.

- Smart infrastructure is the system of the city's physical and organizational structures like its buildings, transportation structures, and other establishments vital to the city's operation.
- Smart society and the public utilize IoT to enhance living, education, healthcare and various societal systems. It also involves socio-economic schemes, public life, social communication, cultural activities, recreation, and tourism [23].
- Smart Mobility implies an intelligent transportation system for both individual citizens and the whole. Smart city vehicles are embedded with computational and communication devices, and vehicles exist on a network with others, which enable vehicles in the city to communicate and be monitored efficiently [24].
- Smart environment ensures the sustainability of a smart city by protecting the environment's quality, responsible management of natural resources, maintaining ecosystem balance, monitoring of economic activity concerning its effect on the environment, and enforcing policies and regulations. Adapting to climate changes, implementing green technology, systematic reduction of pollutants, development of environmentally beneficial technologies, and efficient resource management also concern the smart environment.
- Smart Governance entails the intelligent management of the smart city and its infrastructure and public. The quality and availability of public service are improved along with the public and transparency of policy decisions.

9.3. Healthcare in Smart City

Smart healthcare is a system within a smart city that leverages technologies like IoT, mobile internet, and cloud to dynamically access healthcare information, create connections among people and organizations related to healthcare, and actively manage the healthcare needs intelligently. Smart healthcare enables effective resource allocation within the healthcare sector and maintains strong interaction between all actors, ensuring that participants get proper services and make rational decisions.

9.3.1 Smart Healthcare Applications

The development of computational technologies is changing the face of healthcare. Sensors of smart cities measure several that can be used to know citizens' conditions at any point in time [25]. Frequent gathering of data and processing helps to get healthcare perpetually smarter. Many services have been proposed to support physicians and specialists' efficient work to help prevent and diagnose diseases and provide necessary treatments and therapy [26]. The following sections can categorize significant applications of smart healthcare:

9.3.1.1 Assisting diagnosis and treatment

Technologies like artificial intelligence and surgical robots make diagnosis and treatment of diseases smarter. Artificial intelligence helps to make decisions about the examined result of certain diseases. The efficacy can exceed human doctors [27, 28]. Machine learning-based systems might be more accurate than experienced physicians in terms of medical imaging. The sensors play their role by working in the beginning stage of data processing. These can gather necessary information about ill persons [29]. IBM's Watson is an intelligent cognitive system that can diagnose diabetes and cancer [30]. This supportive clinical system helps doctors give proper treatment to the patients and reduces misdiagnosis. A smart diagnosis system helps develop personalized treatment plans [31]. The Invention of surgical robots is another enticing and effective addition in assisting medical operations and treatment [32].

9.3.1.2 Health management

Wearable smart devices and smartphones are embedded with sensors are used for patient’s medical condition monitoring. These devices can measure movement and rotation respectively in three dimensions relative to the device. Integrating Wifi, GPS and GSM sources can track an individual's location to detect whether they are at or away from home. The compass can find the heading and the barometers can detect the altitude. Many smart devices are equipped with cameras and microphones that can sense people's density at a particular place. Components such as LEDs and photodiodes in smartwatches use light to measure the amount of blood flowing past a patient's wrist and determine heart rate accordingly while connecting smartphones with glucose meters to monitor blood sugar levels. Body area networks (BAN) can be created by putting sensors on or close to the physical body. It uses small sensors and control units to capture data. There are special sensors to monitor rheumatoid arthritis, heart arrhythmias, sleep apnea, cranial pressure, etc. [33]. For example, the electrochemical glucose sensor is popular in diagnosing diabetes [34].

9.3.1.3 Healthcare based on smart homes

Smart homes' role in smart healthcare is mainly divided into two parts: Firstly, health monitoring and home automation. The temperature sensor is an ambient sensor that can measure room temperature and humidity. Passive infrared (PIR) sensors can measure heat-based movement and ambient light levels. Similarly, magnetic sensors can detect the open and close action of the door. Bluetooth low energy sensors or Radio-frequency identification (RFID) can also detect object movement. Some other ambient sensors such as CO_2, power, water, and light sensors can provide outstanding services by collecting data related to patients' health conditions without healthcare professionals' needs. Secondly, patients can use various smart health applications and web services for self-monitoring purpose [35,36].

9.3.1.4 Virtual assistant

In smart healthcare, virtual assistants work using algorithms that communicate using speech recognition techniques. The inherent operations largely depend on big data. For patients, a virtual assistant works on a smart device that searches for the best healthcare service-related information by taking voice command as an input. Virtual assistants help doctors with managing and monitoring medical processes. more efficiently based on patient's medical information, which saves more time. In medical institutions, it can be used to save workforce and reduce human labor.

9.3.1.5 Smart hospitals

A smart hospital system can resolve the issue of the limited number of hospital staff and employees. IoT optimized environments can automate processes and introducing new features. Smart hospitals uses state of the art technologies for administrative procedure, doctors schedule management, staff management, appointment system, advance booking etc. Moreover, these types of hospitals can have a wholistic integration approach with the healthcare sensors for better efficiency [30]. Moreover, these hospitals can have state of the art research facility which can be very useful for on the spot use case research [37,38].

Several other present-day smart health features and countermeasures have been discussed in Table 9.1 below.

Table 9.1: Recent Advances of smart healthcare

References	**Years**	**Features**
Kumar et al. [39]	2017	patient health monitoring using non-invasive sensors; Thingspeak android app for doctors or paramedical staff;
Mshali et al. [40]	2018	Adaptive context-aware e-health monitoring system for old aged and isolated persons living alone; Health state prediction;

Wan et al. [41]	2018	IoT-cloud-based approach; Real-time and ubiquitous monitoring;
Mshali et al. [42]	2018	Analysis of human behavior; Smart environment for elderly and dependent people;
Kang et al. [43]	2018	Cloud computing and blockchain for actively monitor patient health conditions; Self-monitoring health state using wearable devices
Kharel et al. [44]	2018	Long Range wireless communication and fog computing for long range connectivity between health monitoring applications;
Kajornkasirat et al. [45]	2018	IoT based healthcare monitoring system using API technology. Web/ mobile application created using SQL, PHP, Java, JavaScript, HTML5, Android Studio.
Albahri et al. [46]	2019	Heterogeneous wearable sensors for real-time health monitoring; Multi-healthcare services;
Puntambekar et al. [47]	2019	Assistive band for health analysis;
Li et al. [48]	2019	Factors affecting acceptance of smart wearables in elders; Tested acceptance model
Islam and Shin [49]	2019	Unmanned Aerial Vehicle in outdoor health monitoring; Usage of blockchain and mobile edge computing
Hartmann et al. [50]	2019	Edge computing techniques in Smart Health; Edge computing data operations; Challenges and future directions
Gahlot et al. [51]	2019	Smart healthcare development in villages and towns; Early disease diagnosis system;
Rajamohanan et al. [52]	2019	Bluetooth Low Energy(BLE) based technology in smart healthcare wearable devices; Comparison of BLE with other wearable device technologies
Rayan et al. [53]	2019	Machine learning in smart health;
Abdellatif et al. [54]	2020	Smart Health management using blockchain and edge computing; Remote monitoring, fast response, epidemic discovery; Secure medical data sharing
Allam and Jones [55]	2020	Virus outbreak from an urban standpoint; Enhanced standardization protocols for increased data sharing
Zghaibeh et al. [56]	2020	Private multi-layered blockchain based Health management; Smart contract and Consensus Mechanism
Meng et al. [57]	2020	Textile based wireless biomonitoring system; noninvasive and comfortable sensor for BAN with high sensitivity
Chen et al. [58]	2020	Zero Trust architecture in 5G smart healthcare for repeated identity authentication, trustworthy dynamic access control

		models, monitoring access behavior, and ensuring real-time security.
Ahmadi-Assalemi et al. [59]	2020	Digital Twins show real time status by matching physical objects in the health industry with digital models for enhanced patient care, risk analysis and obtaining precision healthcare.
Wang et al. [60]	2020	Consortium blockchain forbids unpermitted access to stored and shared data; Proxy Re-encryption dynamically controls third party access while GCN recognizes malicious nodes.
Tanwar et al. [61]	2020	Healthcare record management using blockchain; improved accessibility of data;
Zhong et al. [62]	2021	Attribute-based strategy for access control, updating attributes, and data encryption in the healthcare domain. It's security is confirmed by a performance check at various security levels and a DBDH assumption
Wu et al. [63]	2021	Edge-based hybrid network system to facilitate data transfer; Extended range for short-range IOT protocols like BLE;
Yang et al. [64]	2021	Optimized data processing and node deployment efficiency in IoT assisted healthcare with end-edge-cloud architecture; maximized intelligence level in medical emergency
Jafar A.Alzubi [65]	2021	Secure healthcare IoT device authentication using block-chain and Lamport Merkle Digital Signature; identification of malicious user behaviour for improved protection of sensitive patient data

9.4. Smart Healthcare Privacy and Security

As the smart healthcare industry heavily relies on smart medical devices, smart hospitals, and other smart services, it is vital to ensure these intelligent healthcare services' securities. Some general security and privacy requirements to ensure protection are authentication, access control, availability, dependability, and flexibility. This section extensively discusses the privacy and security vulnerabilities associated with the intelligent healthcare system and highlights the importance of employing recently developed and improved security measures.

9.4.1 Denial of Service

In this type of attack, intruders exploit the targeted IoMT device or system by flooding the system's data transmission channel with undesired traffic. The attack disrupts the functionality of the IWMDs or deactivate the entire healthcare system as well as block access to emergency medical facilities and its intended users (patients or healthcare providers). The cyber threats associated are deletion and alteration of a patient's critical health data and the insertion of false health information before being passed on to the receiver's end (hospitals, healthcare professionals). This form of security breaches can pose a significant threat to a patient's life. It can result in improper treatment of the patient, wrong prescription by a healthcare provider, false emergency patient alarms, and can even show an inaccurate status of the patient. In health organizations, such attacks apply to implantable devices (insulin pumps, cardiac monitors, pacemakers), wearable health monitoring technologies (Fitbit trackers), and on-site medical equipment (PET scanner, MRI machines, X-ray machines, Dialysis machines) [66, 67]. Some variants of DoS attacks have been discussed below:

9.4.1.1 Jamming attacks

Among some of the physical layer's common attacks are Jamming attacks in which malicious jamming nodes are used to intercept authorized wireless communications between medical sensors in WBAN systems. The attacker's radio frequencies interfere with the RF signals of the WBAN nodes which reduces the Signal-to-noise ratio (SNR). The severity of this attack varies depending upon the attacker's knowledge about the network. The attacker may cause functionality disturbance in a minor portion of the network or even interruption in the entire network. Due to WBAN being a small network, it is at a greater risk of getting blocked [68 – 70].

9.4.1.2 Node Tampering Attacks

Another subset of DoS attacks in the physical layer is tampering attacks. The attackers exploit vulnerabilities in wearable medical sensors, implantable technologies, and other hospital devices to extract patients' confidential health data and modify them via radiofrequency electromagnetic waves.

9.4.1.3 Data Collision Attacks

These attacks mostly occur in the data link layer when two or more terminal nodes transmit data packets, causing packet collisions. The cyber attacker may intentionally escalate the number of collisions by frequently transferring messages via the network channel. This leads to a breakdown of communication and network performance deterioration [71].

9.4.1.4 Exhaustion attack

The aim of this DoS attack in the link layer is to consume the battery resources. A self-sacrificing node may exploit the vulnerabilities of the MAC layer protocols such as Request-To-Send (RTS) and Clear-To-Send (CTS) signals in the IEEE 802.11 MAC protocols. The transmitter node transfers an RTS data packet requesting access to the data transmission channel. The receiver node (victim) responds with a CTS data packet allowing the transmitter node to transmit it. This continuous packet transmission via the transmission channel causes frequent packet collisions and keeps the channel busy. Thus, exhausting the energy resources of the battery.

9.4.1.5 Vampire attacks

It is also called resource depletion attacks, target the medical sensor nodes' batteries by dissipating their power resources, decreasing their expected lifetime. This form of energy-draining DoS attacks in the network layer uses malicious nodes to generate and transfer protocol compliant messages. It consumes more power by routing and processing (by producing longer routes and constructing loops) than legitimate nodes that transfer messages of the same size to the same destination. This increase in energy consumption arises from the Vampire nodes modifying the packets' header information before bombarding them on to the victim nodes to add extra load. Moreover, these attacks are not easily detectable and preventable as they are protocol-independent. [72]

9.4.1.6 Black hole

This type of DoS attack in the network layer involves adversary nodes taking advantage of the routing protocol. The adversary nodes can then misroute all the data traffic towards themselves before consuming them. For instance, when an attacker node receives a Route REQuest, RREQ data packet from a source node, it sends a Route REPly, RREP data packet making a false claim of having the shortest route to the destination node. Once the source node transfers its packet to the attacker node, the packets are dropped or destroyed instead of being forwarded to their expected destination without notifying the source node [73].

9.4.1.7 TCP SYN Flooding attack

This one is a transport layer attack that utilizes the three-way handshake mechanism to send a spoofed package to its targeted server. This is implemented when the victim responds with a SYN/ACK packet placing the connection request in a queue. The SYN/ACK packet is transmitted to another host instead of the original client, so it does not respond as it did not send SYN packets. Hence the adversary does not complete the third step of the mechanism. In this way, the adversary can iteratively send numerous SYN packets causing its target to open several TCP connections and respond to them. So, the victim cannot handle any new incoming requests as its queue is already filled with large volumes of partially-open TCP connections. This causes the depletion of memory resources by reaching a threshold limit [74].

CoAP based enhanced DTLS scheme, Software Defined Networking based defense, learning automata-based approach, and some machine learning techniques such as deep learning are some countermeasures against DoS and DDoS. A scheme called Secure-DAD can be used against DoS attacks in IPv6 Duplicate Address Detection, DAD processes [75-78]. Some blockchain approaches can also be used against these attacks. Combining IoMT devices with Ethereum helps minimize the risk of DDoS attacks [79, 80].

9.4.2 Spyware and Worm Attacks

Spyware, a malware class, is used to gather confidential ePHI of patients without their knowledge and relay them to third party entities or sell them for the attacker's gain. Its malicious activities involve spying on their targets (healthcare sectors) via covet surveillance and monitoring their online activities to steal sensitive information. Among some of the most disastrous malware attacks are Worm attacks which can easily exploit the vulnerabilities in IWMDs as the manufacturers of these devices do not spend sufficient resources and time on strengthening their security. The worms can then replicate vertically to extract confidential information or even destroy the targeted IoMT devices leading to the loss of crucial data that can be life-threatening to devices' users. Moreover, integrating these malicious attacks with other forms of malware attacks (Ransomware, Botnet, Trojan) can infect the entire medical network. Possible solutions are anti-virus, anti-spyware, anti-malware, intrusion detection, and machine learning algorithms [81, 82].

9.4.3 Ransomware

These malware attacks are launched towards the health industry via phishing emails, malicious links, attachments, and mail advertisements. A series of steps are carried out to implement the encryption key successfully. Firstly, the malicious program fixes the external IP address, deletes copies, creates a single ID, etc. Next, important patient files and hospital documents are searched within the system with extensions like .docx, .pptx, .pdf, .jpg, .png, .xlsx. They are then shifted to different locations, renamed, and their original extensions are changed to ransomware extensions such as .crypto, _crypt, locked, RDM, RRK etc the original files are deleted. Finally, these files are made inaccessible by the process of encryption in crypto-ransomware or locking in locker-ransomware and the victimized hospitals are threatened to pay a ransom fee to unlock their files. The attacker may increment their financial claim, misuse or delete vital health records, appointment and surgery schedules, and crucial hospital documents if the ransom fee is not paid in time. As several patients' health records are exposed to the attacker and hospitals have sufficient financial resources, they are more likely to pay the ransom. Hence, making healthcare industries more vulnerable to ransomware attacks. Honeypot, Intrusion Detection Honeypot (IDH), and machine learning approaches are some effective defense mechanisms to deal with the growing concerns of ransomware [83-85].

9.4.4 Eavesdropping

Eavesdropping is when an illegitimate entity secretly intercepts the user's sensitive information (patient-related information or their EMR) without their knowledge or permission. The stolen information may be used to perform malevolent activities leading to privacy breaches. This attack acts as an access point prerequisite to implement many other attacks such as spyware, MITM, side-channel attacks, etc. Eavesdropping attacks can be subdivided into Passive Eavesdropping. The attacker can scan to detect which medical devices (IWMDs and on-site medical equipment) are connected to the wireless access points, and Active Eavesdropping. The attacker can spy on the data sent and received while in transit. These attacks are difficult to diagnose as no deletion or modification of data is involved and also no issues are detected in the network transmission channel. Encryption techniques such as SecureVibe, and lightweight key agreement and mutual authentication mechanisms along with a software tool, ProVerif can help to mitigate these attacks and also several other attacks like spoofing, jamming, replay attacks, etc [86, 87]

9.4.5 Man In The Middle

In healthcare, MITM involves Protected Health Information. PHI is transferred from one point to another between two legitimate parties (between patient and cloud, between cloud and smart healthcare industry, or between IWMDs and on-site medical devices). They think they are directly communicating with each other. An unauthorized entity who hacks the data secretly during the transmission process decrypts it, reviews it and then re-encrypts it before passing it on to the receiver (passive attack). The hacked data can be selectively altered, duplicated, manipulated, or even have malicious codes injected into them (active attack) to be used against the attacker's victims for the attacker's benefit, such as obtaining sensitive medical information of patients. Some effective countermeasures are advanced ECG based authentication techniques that eliminate the acoustic interferences unlike traditional ECGs while preserving privacy [88-90]

9.4.6 Side Channel attacks

The adversary utilizes side-channel information such as execution time of operations, fault frequencies, and power-related data to obtain IoT encryption key. Similarly, forged signals are introduced in an EM Injection attack, which are strong enough to dominate the original signals generated by implantable electronic devices. Another subset of side-channel attacks is Differential Power Analysis, DPA attack that utilizes the statistical data to overcome the cryptographic barriers and gain access to the desired implantable or wearable devices. When a smartwatch is infected with some malicious software, and a smartphone comes nearby, side-channel keystroke inference attacks can occur. Motion sensors like accelerometers and gyroscopes in the infected smartwatch can detect the wrist motions while tapping each keystroke in the smartphone keypad. Solutions include advanced cryptographic techniques such as Elliptic Curve Cryptography, ECC, software-based solutions such as TinySec. To further prevent these close-range attacks, patients may wear wrist bands or carry cards with secret keys of their IWMDs imprinted on them, or even have the keys tattooed on to their skin using ultraviolet-reactive pigmentation [91-94].

9.5. Challenges and Future Research Direction of Smart City Healthcare

Implementing smart healthcare systems in the smart city poses challenges and has limitations outside of the privacy and security dimension. Technological, financial, psychological and administrative demands are required to be met when adopting smart healthcare [95], alongside the challenges they present. These challenges are exhibited in the development of proper smart healthcare architecture, raising the public awareness and engagement and interoperability with other pillars on a macro-level and improving accessibility, data handling, efficiency etc. of healthcare IoT devices and sensors micro-level. This section aims to present the challenges and opportunities in the technological domain.

9.5.1 Wearable Technology Challenges

Sensors and other connected devices are fundamental blocks of a smart healthcare system and pose their limitations. Wearable devices employed in healthcare require environments that support ambient intelligence and in which heterogeneous systems can operate simultaneously [96]. Body area network sensors have complexities brought on by their need to be operated and maintained by humans. The challenges in normalizing this technology lie in making the devices more comfortable for humans, easy to operate, and secure [97] [98]. The wearable sensors also require more accuracy and fault tolerance to be on par with hospital-grade equipment. There is a tradeoff between the accuracy and energy efficiency and wearability of sensors currently available, and finds reducing the effect of motion on sensors such as the respiratory rate and pulse sensors is a workable area to improve accuracy [99]. Applying encryption on healthcare wearable devices is also an important issue.

9.5.2 Smart Healthcare Data Challenges

Another essential side of smart healthcare, which poses several challenges and also numerous research scopes and future opportunities, is big data. The lack of a standardized data format and transfer protocol increases data handling complexity [100]. Researchers have also pointed towards the disparity in progress between data storage and data processing, which is less developed. Cloud-based algorithms are emphasized when it comes to big data processing. The sensitive nature of healthcare data also warrants addressing issues in transmission. The long route of data transmission, through multiple stations, affects the transmitted data due to noise and poses the challenge of developing effective noise removal techniques.

9.5.3 Recommendations and Opportunities

The smart healthcare system should move towards accurate, cost effective, personalized and efficient service provider [101,102]. Recently, blockchain technology integration into smart cities is being researched to ensure more robust security [103, 104]. As these superior technologies integrate with healthcare to form a smart healthcare system, many research and development opportunities arise. Recent research directions and recommendations are outlined in this section.

9.5.3.1 Specialized Algorithms and Machine Learning in Smart Healthcare

Machine learning and development of algorithms for specific purposes are heavily recommended in recent papers, and there are numerous scopes of application of ML in smart healthcare. For diagnostics, the researchers identified clustering and logistic regression algorithms. Application of machine learning algorithms on signal processing on ECG monitoring to reduce supervision costs and the development of optimization algorithms to minimize wearable devices' energy consumption is recommended in the paper. Reference [105] uses multilayered extreme machine learning to identify human activities, which can have implications on health monitoring applications' scope. Machine learning techniques should also be developed to uphold the quality of cloud services in healthcare [106].

9.5.3.2 Energy Harvesting for Wearable Devices

One rapidly growing area in the development of wearable sensors is energy harvesting. Adapting the energy harvesting mechanisms of autonomous wireless sensors for very low power and lightweight sensors employed in smart health applications like body area networks would significantly improve them. Kinetic energy-based energy harvesting [107] is more popular, but its scope does not encompass all wearable devices, for which thermoelectric energy harvesting may be explored [108], [109]. Reference [110] presents experimental validation for piezoelectric energy harvesting, which can power wearables through the human knee movements. Research is also being done to harvest low-frequency biomechanical movements using nanogenerators [111][112]. Reference [113] discusses a possible radiofrequency energy harvester and storing system for wearable sensors.

9.5.3.3 Wearable Device Development

Wearable devices have a broad range of applications and demand usage-specific technologies besides common ones. Implementation of identification and localization mechanisms into wearable devices without affecting their lightweight and ensuring proper privacy measures is one necessary area to research. Body area networks with inbuilt drug pumps and other closed-loop systems, for example, necessitate the development of proper user identification [97]. Near field communication and RFIDs can be utilized in smart health applications to localize users in small areas such as elderly care homes [114]. Encryption of data from wearable devices is another complex area with the scope of research. For cloud-based smart healthcare security, the paper [99] recommends an Attribute-Based Encryption (ABE) and fully homomorphic encryption (FHE) hybrid scheme which would be lightweight implementing on wearable devices. To enhance the response time and critical situating management, Tuli et al. [106] propose integrating various frameworks such as sensor networks, serverless computing, data analytics etc. and shifting computation to the wearable devices. The researchers also put forward quantum computing, targeted operating systems, 6G, processing-in-memory etc. as future research directions in smart healthcare.

9.5.3.4 Big Data Analytics

The big data of smart healthcare also opens a myriad of opportunities for research, application development, and healthcare improvement. As the data provides a clearer picture of critical situations, more adept intervention methods can be used. Analysis of aggregate data will be crucial in solving medical questions and a quicker and more accurate diagnosis of diseases and identifying the most effective treatments. Health threat identification, epidemics detection and management can be streamlined through historical and globally aggregated health data [96].

9.5.3.5 Smartphone Applications for Smart Healthcare

Smartphone-based healthcare tools are a rising wave of applications that utilize and generate big data of smart healthcare. With billions of individuals operating smartphones, the P4 goal of healthcare is getting closer to actualization. Smartphones present a versatile platform, and many research opportunities exist in the development of smartphone-based health monitoring. The area is being explored by recent researches such as smartphone ECG monitoring[115], respiratory monitoring, testing for respiratory disease symptoms[116], oral health monitoring using noninvasive periodontal diagnosis [117], and so on. There is immense potential for providing mental healthcare through smartphones. User engagement issues need to be resolved through innovative means to improve the usage of these applications [118]; research into improving these applications' trustworthiness and transparency could transform user acceptance [119,120]. Smartphones are becoming the apex of IoT networks in healthcare. Their already massive users and research into smoother integration with cloud and improved processing of the enormous could revolutionize smart healthcare.

9.6. Conclusion

This chapter discuss the smart healthcare based on smart city perspectives including the application of IoT in smart healthcare applications. Healthcare is a basic human need and one of the most crucial sector to focus. The recent pandemic has hit countries worldwide in unprecedented ways and has asserted the importance of an intelligent healthcare system. Smart cities should have vital healthcare and preventive ones that utilize the constant stream of data generated by its citizens to identify patterns of diseases and the effectiveness of treatments and therapies. Attacks on smart healthcare can cripple the total system. Due to the attacks, significant data will be lost and personal data will be at risk. Since health data is one of the most sensitive data falling it into the wrong had can bring catastrophic effects. For this reason, possible countermeasures are needed. These are discussed in this paper.

The scope of future research in smart healthcare is extensive. Smart health applications require better-specialized algorithms and integration of machine learning for more intelligent systems. Wearable devices and BANs need improved energy efficiency and added features without compromising lightweights or security. The big data of healthcare also opens opportunities for research into data operations targeted for healthcare and efficient storing mechanisms. The importance and exigency of research into smart healthcare and the plethora of opportunities present make it a prime research area. A foundation for understanding smart healthcare in smart cities has been laid out in this paper in recent years.

References

[1] F. Cirillo, D. Gómez, L. Diez, I. Elicegui Maestro, T. B. J. Gilbert and R. Akhavan, "Smart City IoT Services Creation Through Large-Scale Collaboration," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5267-5275, June 2020, doi: 10.1109/JIOT.2020.2978770.

[2] C. C. de Alba, C. C. de Alba, J. Haberleithner, and M. M. R. López, "Creative Industries in the Smart City,"Handbook of Research on Entrepreneurial Development and Innovation Within Smart Cities," pp. 107–126, 2017, doi: 10.4018/978-1-5225-1978-2.ch006.

[3] Laurini, R. (2020). A primer of knowledge management for smart city governance. Land Use Policy, 104832, DOI: 10.1016/j.landusepol.2020.104832.

[4] M. G. Vaquero and J. M. Saiz-Alvarez, "Smart Cities in Spain – Policy, Sustainability, and the National Plan," Economic Modeling, Analysis, and Policy for Sustainability. pp. 266–283, 2016, doi: 10.4018/978-1-5225-0094-0.ch014.

[5] B.-J. Park et al., "Long-Term Warming Trends in Korea and Contribution of Urbanization: An Updated Assessment," Journal of Geophysical Research: Atmospheres, vol. 122, no. 20. pp. 10,637–10,654, 2017, doi: 10.1002/2017jd027167.

[6] Roopa M.S., Santosh Pattar, Rajkumar Buyya, Venugopal K.R., S.S. Iyengar, L.M. Patnaik, Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions, Computer Communications,Volume 139,2019,Pages 32-57,ISSN 0140 3664,DOI:10.1016/j.comcom.2019.03.009.

[7] V. E. Balas, V. K. Solanki, R. Kumar, and M. Khari, "Internet of Things and Big Data Analytics for Smart Generation", Springer, vol. 154, 2018, doi: 10.1007/978-3-030-04203-5.

[8] Y. J. Fan, Y. H. Yin, L. Da Xu, Y. Zeng, and F. Wu, "IoT-Based Smart Rehabilitation System," IEEE Transactions on Industrial Informatics, vol. 10, no. 2. pp. 1568–1577, 2014, doi: 10.1109/tii.2014.2302583.

[9] L. C. Câmara Gradim, M. Archanjo José, D. Marinho Cezar da Cruz and R. de Deus Lopes, "IoT Services and Applications in Rehabilitation: An Interdisciplinary and Meta-Analysis

Review," in IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 28, no. 9, pp. 2043-2052, Sept. 2020, doi: 10.1109/TNSRE.2020.3005616.

[10] S.-H. Chang, R.-D. Chiang, S.-J. Wu, and W.-T. Chang, “A Context-Aware, Interactive M-Health System for Diabetics,” IT Professional, vol. 18, no. 3. pp. 14–22, 2016, doi: 10.1109/mitp.2016.48.

[11] G. Wolgast, C. Ehrenborg, A. Israelsson, J. Helander, E. Johansson, and H. Manefjord, “Wireless Body Area Network for Heart Attack Detection [Education Corner],” IEEE Antennas and Propagation Magazine, vol. 58, no. 5. pp. 84–92, 2016, doi: 10.1109/map.2016.2594004.

[12] R. E. Hall, B. Bowerman, J. Braverman, J. Taylor, H. Todosow, and U. Von Wimmersperg, "The vision of a smart city," Brookhaven National Lab., Upton, NY (US), BNL-67902; 04042, Sep. 2000.

[13] C. Harrison, “Roads to Smarter Cities,” Concept-Oriented Research and Development in Information Technology. pp. 55–69, 2014, doi: 10.1002/9781118753972.ch4.

[14] Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. (2007), "Smart cities: ranking of European medium-sized cities", Vienna UT, Jan. 2007
.
[15] J. M. Eger, “Smart Growth, Smart Cities, and the Crisis at the Pump A Worldwide Phenomenon,” I-WAYS, Digest of Electronic Commerce Policy and Regulation, vol. 32, no. 1. pp. 47–53, 2009, doi: 10.3233/iwa-2009-0164.

[16] U. N. D. of E. A. S. Affairs and United Nations Department of Economic and Social Affairs, “World Urbanization Prospects: The 2018 Revision.” 2019, doi: 10.18356/b9e995fe-en.

[17] M. Chen, “Towards smart city: M2M communications with software agent intelligence,” Multimed. Tools Appl., vol. 67, no. 1, pp. 167–178, Nov. 2013, doi: 10.1007/s11042-012-1013-4

[18] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han and R. Buyya, "BlockSDN: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications," in IEEE Network, vol. 34, no. 2, pp. 83-91, March/April 2020, doi: 10.1109/MNET.001.1900151.

[19] B. N. Silva, M. Khan, and K. Han, “Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities,” Sustainable Cities and Society, vol. 38. pp. 697–713, 2018, doi: 10.1016/j.scs.2018.01.053.

[20] Haque, A. B., &amp; Bhushan, B. (2021). Security Attacks and Countermeasures in Wireless Sensor Networks. Integration of WSNs into Internet of Things, 17-43. doi:10.1201/9781003107521-2

[21] Kandris, D., Nakas, C., Vomvas, D., &amp; Koulouras, G. (2020). Applications of wireless sensor networks: An up-to-date survey. Applied System Innovation, 3(1), 14. doi:10.3390/asi3010014

[22] M. Wazid, A. K. Das, R. Hussain, G. Succi, and Joel J P, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," Journal of Systems Architecture, vol. 97. pp. 185–196, 2019, doi: 10.1016/j.sysarc.2018.12.005.

[23] U. Gretzel, H. Werthner, C. Koo, and C. Lamsfus, "Conceptual foundations for understanding smart tourism ecosystems," Computers in Human Behavior, vol. 50. pp. 558–563, 2015, doi: 10.1016/j.chb.2015.03.043.

[24] A. Kirimtat, O. Krejcar, A. Kertesz, and M. Fatih Tasgetiren, "Future Trends and Current State of Smart City Concepts: A Survey," IEEE Access, vol. 8. pp. 86448–86467, 2020, doi: 10.1109/access.2020.2992441.

[25] L. Bedogni, L. Bononi, M. Di Felice, A. D'Elia, and T. S. Cinotti, "A Route Planner Service with Recharging Reservation: Electric Itinerary with a Click," IEEE Intelligent Transportation Systems Magazine, vol. 8, no. 3. pp. 75–84, 2016, doi: 10.1109/mits.2016.2573418.

[26] A. Page et al., "SUPPORT SYSTEMS FOR HEALTH MONITORING USING INTERNET-OF-THINGS DRIVEN DATA ACQUISITION," Services Transactions on Services Computing, vol. 4, no. 4. pp. 18–34, 2016, doi: 10.29268/stsc.2016.4.4.2.

[27] J. Dhar and A. Ranganathan, "Machine learning capabilities in medical diagnosis applications: computational results for hepatitis disease," International Journal of Biomedical Engineering and Technology, vol. 17, no. 4. p. 330, 2015, doi: 10.1504/ijbet.2015.069398.

[28] A. Esteva et al., "Dermatologist-level classification of skin cancer with deep neural networks," Nature, vol. 542, no. 7639. pp. 115–118, 2017, doi: 10.1038/nature21056.

[29] M. Jindal, J. Gupta, and B. Bhushan, "Machine learning methods for IoT and their Future Applications," 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). 2019, doi: 10.1109/icccis48478.2019.8974551.

[30] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," Global Health Journal, vol. 3, no. 3. pp. 62–65, 2019,

doi: 10.1016/j.glohj.2019.07.001.

[31] Toğaçar, M., Özkurt, K. B., Ergen, B., & Cömert, Z. (2020). BreastNet: A novel convolutional neural network model through histopathological images for the diagnosis of breast cancer. Physica A: Statistical Mechanics and its Applications, 545, 123592. DOI: 10.1016/j.physa.2019.123592

[32] B. S. Peters, P. R. Armijo, C. Krause, S. A. Choudhury, and D. Oleynikov, "Review of emerging surgical robotic technology," Surgical Endoscopy, vol. 32, no. 4. pp. 1636–1655, 2018, doi: 10.1007/s00464-018-6079-2.

[33] D. J. Cook, G. Duncan, G. Sprint, and R. Fritz, "Using Smart City Technology to Make Healthcare Smarter," Proc. IEEE Inst. Electr. Electron. Eng., vol. 106, no. 4, pp. 708–722, Apr. 2018, doi: 10.1109/JPROC.2017.2787688.

[34] J. Y. Lucisano, T. L. Routh, J. T. Lin, and D. A. Gough, "Glucose Monitoring in Individuals With Diabetes Using a Long-Term Implanted Sensor/Telemetry System and Model," IEEE Trans. Biomed. Eng., vol. 64, no. 9, pp. 1982–1993, Sep. 2017, doi: 10.1109/TBME.2016.2619333.

[35] A. O. Akmandor and N. K. Jha, "Keep the Stress Away with SoDA: Stress Detection and Alleviation System," IEEE Transactions on Multi-Scale Computing Systems, vol. 3, no. 4. pp. 269–282, 2017, doi: 10.1109/tmscs.2017.2703613.

[36] J. Redfern, "Smart health and innovation: facilitating health-related behaviour change," Proceedings of the Nutrition Society, vol. 76, no. 3. pp. 328–332, 2017, doi: 10.1017/s0029665117001094.

[37] "Oncologists Partner with Watson on Genomics," Cancer Discovery, vol. 5, no. 8. pp. 788–788, 2015, doi: 10.1158/2159-8290.cd-nb2015-090.

[38] F. Zhong et al., "Artificial intelligence in drug design," Science China Life Sciences, vol. 61, no. 10. pp. 1191–1204, 2018, doi: 10.1007/s11427-018-9342-2.

[39] S. P. Kumar, V. R. R. Samson, U. B. Sai, P. L. S. D. M. Rao, and K. K. Eswar, "Smart health monitoring system of patient through IoT," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, Tamilnadu, India, pp. 551–556, Feb. 2017, doi: 10.1109/I-SMAC.2017.8058240.

[40] H. Mshali, T. Lemlouma, and D. Magoni, "Adaptive monitoring system for e-health smart

homes," Pervasive Mob. Comput., vol. 43, pp. 1–19, Jan. 2018, doi: 10.1016/j.pmcj.2017.11.001

[41] J. Wan et al., "Wearable IoT enabled real-time health monitoring system," Eurasip J. Wirel. Commun. Network., vol. 2018, no. 1, p. 59, Dec. 2018, doi: 10.1186/s13638-018-1308-x

[42] H. Mshali, T. Lemlouma, M. Moloney, and D. Magoni, "A survey on health monitoring systems for health smart homes," Int. J. Ind. Ergon., vol. 66, pp. 26–56, Jul. 2018, doi: 10.1016/j.ergon.2018.02.002

[43] M. Kang, E. Park, B. H. Cho, and K.-S. Lee, "Recent Patient Health Monitoring Platforms Incorporating Internet of Things-Enabled Smart Devices," Int. Neurourol. J., vol. 22, no. Suppl 2, pp. S76–82, Jul. 2018, doi: 10.5213/inj.1820corr.001

[44] J. Kharel, H. T. Reda, and S. Y. Shin, "Fog Computing-Based Smart Health Monitoring System Deploying LoRa Wireless Communication," IETE Tech. Rev., vol. 36, no. 1, pp. 69–82, Jan. 2018, doi: 10.1080/02564602.2017.1406828

[45] S. Kajornkasirat, N. Chanapai, and B. Hnusuwan, "Smart health monitoring system with IoT," in 2018 IEEE Symposium on Computer Applications &amp; Industrial Electronics (ISCAIE), Penang, pp. 206–211, Apr. 2018, doi: 10.1109/ISCAIE.2018.8405471

[46] A. S. Albahri et al., "Based Multiple Heterogeneous Wearable Sensors: A Smart Real-Time Health Monitoring Structured for Hospitals Distributor," IEEE Access, vol. 7, pp. 37269–37323, 2019, doi: 10.1109/ACCESS.2019.2898214.

[47] V. Puntambekar, S. Agarwal, and P. Mahalakshmi, "Dynamic Monitoring of Health Using Smart Health Band: SocProS 2018, Volume 2," in Soft Computing for Problem Solving, vol. 1057, Springer Singapore, 2020, pp. 453–462, doi: 10.1007/978-981-15-0184-5_39.

[48] J. Li, Q. Ma, A. H. Chan, and S. S. Man, "Health monitoring through wearable technologies for older adults: Smart wearables acceptance model," Appl. Ergon., vol. 75, pp. 162–169, Feb. 2019, doi: 10.1016/j.apergo.2018.10.006.

[49] A. Islam and S. Y. Shin, "BHMUS: Blockchain Based Secure Outdoor Health Monitoring Scheme Using UAV in Smart City," in 2019 7th International Conference on Information and Communication Technology (ICoICT), Kuala Lumpur, Malaysia, Jul. 2019, pp. 1–6, doi: 10.1109/ICoICT.2019.8835373.

[50] M. Hartmann, U. S. Hashmi, and A. Imran, "Edge computing in smart health care systems: Review, challenges, and research directions," Trans Emerging Tel Tech, vol. 71, p. 503, Aug.

2019, doi: 10.1002/ett.3710.

[51] S. Gahlot, S. R. N. Reddy, and D. Kumar, “Review of Smart Health Monitoring Approaches With Survey Analysis and Proposed Framework,” IEEE Internet Things J., vol. 6, no. 2, pp. 2116–2127, Apr. 2019, doi: 10.1109/JIOT.2018.2872389.

[52] D. Rajamohanan, B. Hariharan, and K. A. Unnikrishna Menon, “Survey on Smart Health Management using BLE and BLE Beacons,” in 2019 9th International Symposium on Embedded Computing and System Design (ISED), Kollam, India, Dec. 2019, pp. 1–5, doi: 10.1109/ISED48680.2019.9096227.

[53] Z. Rayan, M. Alfonse, and A.-B. M. Salem, “Machine Learning Approaches in Smart Health,” Procedia Comput. Sci., vol. 154, pp. 361–368, Jan. 2019, doi: 10.1016/j.procs.2019.06.052.

[54] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, and A. Refaey, “ssHealth: Toward Secure, Blockchain-Enabled Healthcare Systems,” IEEE Netw., vol. 34, no. 4, pp. 312–319, Jul. 2020, doi: 10.1109/MNET.011.1900553.

[55] Z. Allam and D. S. Jones, “On the Coronavirus (COVID-19) Outbreak and the Smart City Network: Universal Data Sharing Standards Coupled with Artificial Intelligence (AI) to Benefit Urban Health Monitoring and Management,” Healthcare (Basel), vol. 8, no. 1, Feb. 2020, doi: 10.3390/healthcare8010046.

[56] M. Zghaibeh, U. Farooq, N. U. Hasan, and I. Baig, “SHealth: A Blockchain-Based Health System With Smart Contracts Capabilities,” IEEE Access, vol. 8, pp. 70030–70043, 2020, doi:10.1109/access.2020.2986789

[57] K. Meng et al., “A Wireless Textile-Based Sensor System for Self-Powered Personalized Health Care,” Matter, vol. 2, no. 4. pp. 896–907, 2020, doi: 10.1016/j.matt.2019.12.025.

[58] B. Chen et al., “A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture,” IEEE Internet of Things Journal. pp. 1–1, 2020, doi: 10.1109/jiot.2020.3041042.

[59] G. Ahmadi-Assalemi et al., “Digital Twins for Precision Healthcare,” Advanced Sciences and Technologies for Security Applications. pp. 133–158, 2020, doi: 10.1007/978-3-030-35746-7_8.

[60] Z. Wang, N. Luo, and P. Zhou, “GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare,” Journal of Parallel and Distributed Computing, vol. 142. pp. 1–12, 2020, doi: 10.1016/j.jpdc.2020.03.004.

[61] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” Journal of Information Security and Applications, vol. 50, p. 102407, Feb. 2020, doi: 10.1016/j.jisa.2019.102407.

[62] H Zhong, Y. Zhou, Q. Zhang, Y. Xu, J. Cui, “An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare,” Future Gener. Comput. Syst., vol. 115, pp. 486–496, Feb. 2021, doi: 10.1016/j.future.2020.09.021.

[63] F. Wu, C. Qiu, T. Wu, and M. R. Yuce, “Edge-Based Hybrid System Implementation for Long-Range Safety and Healthcare IoT Applications,” IEEE Internet of Things Journal. pp. 1–1, 2021, doi: 10.1109/jiot.2021.3050445.

[64] Z. Yang, B. Liang and W. Ji, "An Intelligent End-Edge-Cloud Architecture for Visual IoT Assisted Healthcare Systems," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3052778.

[65] J. A. Alzubi, “Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare,” Comput. Commun., Feb. 2021, doi: 10.1016/j.comcom.2021.02.002.

[66] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, “IoT Smart Health Security Threats,” 2019 19th International Conference on Computational Science and Its Applications (ICCSA). 2019, doi: 10.1109/iccsa.2019.000-8.

[67] Hassija, V., Chamola, V., Bajpai, B. C., & Zeadally, S. (2020). Security Issues in Implantable Medical Devices: Fact or Fiction?. Sustainable Cities and Society, 102552. doi: 10.1016/j.scs.2020.102552

[68] S. Alam and D. De, “Analysis of Security Threats in Wireless Sensor Network,” International Journal of Wireless &amp; Mobile Networks, vol. 6, no. 2. pp. 35–46, 2014, doi: 10.5121/ijwmn.2014.6204.

[69] H. Habibzadeh and T. Soyata, “Toward Uniform Smart Healthcare Ecosystems: A Survey on Prospects, Security, and Privacy Considerations,” Connected Health in Smart Cities. pp. 75–112, 2020, doi: 10.1007/978-3-030-27844-1_5.

[70] P. Kumar and H.-J. Lee, “Security issues in healthcare applications using wireless medical sensor networks: a survey,” Sensors , vol. 12, no. 1, pp. 55–91, 2012, doi: 10.3390/s120100055

[71] I. Ahmed and A. Mousa, “Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services,” International Journal of Advanced Computer Science and Applications, vol. 7, no. 9. 2016, doi: 10.14569/ijacsa.2016.070933.

[72] M. K. Sharma and B. K. Joshi, “Detection &amp; prevention of vampire attack in wireless sensor networks,” in 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC), Indore, Aug. 2017, pp. 1–5, doi: 10.1109/ICOMICON.2017.8279174.

[73] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, “A survey of black hole attacks in wireless moile ad hoc networks,” Human-centric Computing and Information Sciences, vol. 1, no. 1. p. 4, 2011, doi: 10.1186/2192-1962-1-4.

[74] R. Latif, H. Abbas, and S. Assar, “Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review,” J. Med. Syst., vol. 38, no. 11, p. 128, Nov. 2014, doi: 10.1007/s10916-014-0128-8.

[75] P. M. Kumar and U. D. Gandhi, “Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application,” The Journal of Supercomputing, vol. 76, no. 6. pp. 3963–3983, 2020, doi: 10.1007/s11227-017-2169-5.

[76] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” Telecommunication Systems, vol. 73, no. 1. pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.

[77] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, “Mitigating loT Device based DDoS Attacks using Blockchain,” Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock’18. 2018, doi: 10.1145/3211933.3211946.

[78] S. Ul and S. Manickam, “Improved Mechanism to Prevent Denial of Service Attack in IPv6 Duplicate Address Detection Process,” International Journal of Advanced Computer Science and Applications, vol. 8, no. 2. 2017, doi: 10.14569/ijacsa.2017.080209.

[79] A. Biswal and B. Bhushan, “Blockchain for Internet of Things: Architecture, Consensus Advancements, Challenges and Application Areas,” 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, Sep. 2019, pp.

1–6, doi: 10.1109/ICCUBEA47591.2019.9129181.

[80] D. Arora, S. Gautham, H. Gupta, and B. Bhushan, “Blockchain-based Security Solutions to Preserve Data Privacy And Integrity,” in 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, Oct. 2019, pp. 468–472, doi: 10.1109/ICCCIS48478.2019.8974503.

[81] “Securing internet of medical things systems: Limitations, issues and recommendations,” Future Gener. Comput. Syst., vol. 105, pp. 581–606, Apr. 2020, doi:10.1016/j.future.2019.12.028

[82] P. M. Shakeel, P. Mohamed Shakeel, S. Baskar, V. R. Sarma Dhulipala, S. Mishra, and M. M. Jaber, “Maintaining Security and Privacy in Health Care System Using Learning Based Deep-Q-Networks,” Journal of Medical Systems, vol. 42, no. 10. 2018, doi: 10.1007/s10916-018-1045-z.

[83] P. Podder, M. R. H. Mondal, S. Bharati, and P. K. Paul, “Review on the Security Threats of Internet of Things,” IJCAI , vol. 176, no. 41, pp. 37–45, Jul. 2020, doi: 10.5120/ijca2020920548.

[84] A. H. Mohammad, “Ransomware Evolution, Growth and Recommendation for Detection,” Modern Applied Science, vol. 14, no. 3. p. 68, 2020, doi: 10.5539/mas.v14n3p68.

[85] S. S. Chakkaravarthy, S. Sibi Chakkaravarthy, D. Sangeetha, M. V. Cruz, V. Vaidehi, and B. Raman, “Design of Intrusion Detection Honeypot Using Social Leopard Algorithm to Detect IoT Ransomware Attacks,” IEEE Access, vol. 8. pp. 169944–169956, 2020, doi: 10.1109/access.2020.3023764.

[86] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, “A Lightweight Mutual Authentication and Key Agreement Scheme for Medical Internet of Things,” IEEE Access, vol. 7. pp. 53922–53931, 2019, doi: 10.1109/access.2019.2912870.

[87] M. Papaioannou et al., “A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT),” Transactions on Emerging Telecommunications Technologies. 2020, doi: 10.1002/ett.4049.

[88] P. Huang, L. Guo, M. Li, and Y. Fang, “Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare,” IEEE Internet of Things Journal, vol. 6, no. 5. pp. 9200–9210, 2019, doi: 10.1109/jiot.2019.2929087.

[89] M. L. Shuwandy et al., “mHealth Authentication Approach Based 3D Touchscreen and Microphone Sensors for Real-Time Remote Healthcare Monitoring System: Comprehensive Review, Open Issues and Methodological Aspects,” Computer Science Review, vol. 38. p. 100300, 2020, doi: 10.1016/j.cosrev.2020.100300.

[90] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, “BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud,” Journal of King Saud University - Computer and Information Sciences, vol. 32, no. 1. pp. 57–64, 2020, doi: 10.1016/j.jksuci.2017.07.001.

[91] J. Deogirikar and A. Vidhate, “Security attacks in IoT: A survey,” 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37, doi: 10.1109/I-SMAC.2017.8058363.

[92] M. Zhang, A. Raghunathan and N. K. Jha, “Trustworthiness of Medical Devices and Body Area Networks,”in Proceedings of the IEEE, vol. 102, no. 8, pp. 1174-1188, Aug. 2014, doi: 10.1109/JPROC.2014.2322103.

[93] A. Maiti, M. Jadliwala, J. He, and I. Bilogrevic, “(Smart)watch your taps,” Proceedings of the 2015 ACM International Symposium on Wearable Computers - ISWC ’15. 2015, doi: 10.1145/2802083.2808397.

[94] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” Egyptian Informatics Journal, vol. 18, no. 2, pp. 113–122, Jul. 2017, doi: 10.1016/j.eij.2016.11.001

[95] G. Postolache, P. S. Girão, and O. Postolache, “Requirements and Barriers to Pervasive Health Adoption,” Pervasive and Mobile Sensing and Computing for Healthcare. pp. 315–359, 2013, doi: 10.1007/978-3-642-32538-0_15.

[96] A. Solanas et al., “Smart health: A context-aware health paradigm within smart cities,” IEEE Communications Magazine, vol. 52, no. 8. pp. 74–81, 2014, doi: 10.1109/mcom.2014.6871673.

[97] E. Jovanov and A. Milenkovic, “Body Area Networks for ubiquitous healthcare applications: opportunities and challenges,” J. Med. Syst., vol. 35, no. 5, pp. 1245–1254, Oct. 2011, doi: 10.1007/s10916-011-9661-x

[98] S. Selvaraj and S. Sundaravaradhan, “Challenges and opportunities in IoT healthcare systems: a systematic review,” SN Applied Sciences, vol. 2, no. 1. 2020, doi: 10.1007/s42452-019-1925-y.

[99] S. B. Baker, W. Xiang, and I. Atkinson, “Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities,” IEEE Access, vol. 5. pp. 26521–26544, 2017, doi: 10.1109/access.2017.2775180.

[100] A. Rizwan et al., “A Review on the Role of Nano-Communication in Future Healthcare Systems: A Big Data Analytics Perspective,” IEEE Access, vol. 6. pp. 41903–41920, 2018, doi: 10.1109/access.2018.2859340.

[101] M. Sagner et al., “The P4 Health Spectrum – A Predictive, Preventive, Personalized and Participatory Continuum for Promoting Healthspan,” Progress in Preventive Medicine, vol. 2, no. 1. p. e0002, 2017, doi: 10.1097/pp9.0000000000000002.

[102] U. Varshney and C. K. Chang, “Smart Health and Well-Being,” Computer , vol. 49, no. 11, pp. 11–13, Nov. 2016, doi: 10.1145/2555810.2555811

[103] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, “Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions,” Wireless Networks. 2020, doi: 10.1007/s11276-020-02445-6.

[104] B. Bhushan, A. Khamparia, K. Martin Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, “Blockchain for smart cities: A review of architectures, integration trends and future research directions,” Sustainable Cities and Society, vol. 61. p. 102360, 2020, doi: 10.1016/j.scs.2020.102360.

[105] M. Chen, Y. Li, X. Luo, W. Wang, L. Wang, and W. Zhao, “A Novel Human Activity Recognition Scheme for Smart Health Using Multilayer Extreme Learning Machine,” Cyber-Enabled Intelligence. pp. 239–258, 2019, doi: 10.1201/9780429196621-12.

[106] S. Tuli et al., “Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions,” Internet Technology Letters, vol. 3, no. 2. p. e145, 2020, doi: 10.1002/itl2.145.

[107] P. Gljušćić, S. Zelenika, D. Blažević, and E. Kamenar, “Kinetic Energy Harvesting for Wearable Medical Sensors,” Sensors , vol. 19, no. 22, Nov. 2019, doi: 10.3390/s19224922.

[108] A. Nozariasbmarz et al., “Review of wearable thermoelectric energy harvesting: From

body temperature to electronic systems," Applied Energy, vol. 258. p. 114069, 2020, doi: 10.1016/j.apenergy.2019.114069.

[109] J.-H. Bahk, H. Fang, K. Yazawa, and A. Shakouri, "Flexible thermoelectric materials and device optimization for wearable energy harvesting," Journal of Materials Chemistry C, vol. 3, no. 40. pp. 10362–10374, 2015, doi: 10.1039/c5tc01644d.

[110] Y. Tuncel, S. Bandyopadhyay, S. V. Kulshrestha, A. Mendez, and U. Y. Ogras, "Towards wearable piezoelectric energy harvesting," Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design. 2020, doi: 10.1145/3370748.3406578.

[111] C. Yan et al., "A linear-to-rotary hybrid nanogenerator for high-performance wearable biomechanical energy harvesting," Nano Energy, vol. 67. p. 104235, 2020, doi: 10.1016/j.nanoen.2019.104235.

[112] Y. Zou, V. Raveendran, and J. Chen, "Wearable triboelectric nanogenerators for biomechanical energy harvesting," Nano Energy, vol. 77. p. 105303, 2020, doi: 10.1016/j.nanoen.2020.105303.

[113] L. M. Borges, R. Chávez-Santiago, N. Barroca, F. J. Velez, and I. Balasingham, "Radio-frequency energy harvesting for wearable sensors," Healthc Technol Lett, vol. 2, no. 1, pp. 22–27, Feb. 2015, doi: 10.1049/htl.2014.0096

[114] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The Internet of Things for Ambient Assisted Living," 2010 Seventh International Conference on Information Technology: New Generations. 2010, doi: 10.1109/itng.2010.104.

[115] M. Faezipour and M. Faezipour, "System Dynamics Modeling for Smartphone-Based Healthcare Tools: Case Study on ECG Monitoring," IEEE Systems Journal. pp. 1–10, 2020, doi: 10.1109/jsyst.2020.3009187.

[116] M. Faezipour and M. Faezipour, "Sustainable Smartphone-Based Healthcare Systems: A Systems Engineering Approach to Assess the Efficacy of Respiratory Monitoring Apps," Sustainability, vol. 12, no. 12. p. 5061, 2020, doi: 10.3390/su12125061.

[117] S. Veeralingam, P. Sahatiya, A. Kadu, V. Mattela, and S. Badhulika, "Direct, One-Step Growth of NiSe2 on Cellulose Paper: A Low-Cost, Flexible, and Wearable with Smartphone Enabled Multifunctional Sensing Platform for Customized Noninvasive Personal Healthcare Monitoring," ACS Applied Electronic Materials, vol. 1, no. 4. pp. 558–568, 2019, doi:

10.1021/acsaelm.9b00022.

[118] J. Torous, J. Nicholas, M. E. Larsen, J. Firth, and H. Christensen, “Clinical review of user engagement with mental health smartphone apps: evidence, theory and improvements,” Evid. Based. Ment. Health, vol. 21, no. 3, pp. 116–119, Aug. 2018, doi: 10.1136/eb-2018-102891

[119] J. Torous and L. W. Roberts, “Needed Innovation in Digital Health and Smartphone Applications for Mental Health: Transparency and Trust,” JAMA Psychiatry, vol. 74, no. 5, pp. 437–438, May 2017, doi: 10.1001/jamapsychiatry.2017.0262

[120] A. B. Haque, A. Muniat, P. R. Ullah and S. Mushsharat, "An Automated Approach towards Smart Healthcare with Blockchain and Smart Contracts," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 250-255, doi: 10.1109/ICCCIS51004.2021.9397158.