Modern Study on Internet of Medical Things (IOMT) Security

Ghada Sultan Aljumaie[1], Ghada Hisham Alzeer[2], Reham Khaild Alghamdi[3]
s44180324, s44181669, s44181022@students.tu.edu.sa
Department of Computer Science
College of Computers and Information Technology
Taif University
Hatim Alsuwat[4]
Hssuwat@uqu.edu.sa
Department of Computer Science
College of Computer and Information Systems
Umm Al Qura University,
Emad Alsuwat[5]
Alsuwat@tu.edu.sa
Department of Computer Science
College of Computers and Information Technology
Taif University

Summary
The Internet of Medical Things (IoMTs) are to be considered an investment and an improvement to respond effectively and efficiently to patient needs, as it reduces healthcare costs, provides the timely attendance of medical responses, and increases the quality of medical treatment. However, IoMT devices face exposure from several security threats that defer in function and thus can pose a significant risk to how private and safe a patient's data is. This document works as a comprehensive review of modern approaches to achieving security within the Internet of Things. Most of the papers cited here are used been carefully selected based on how recently it has been published. The paper highlights some common attacks on IoMTs. Also, highlighting the process by which secure authentication mechanisms can be achieved on IoMTs, we present several means to detect different attacks in IoMTs

Key words:
Internet of Medical Things, IoMT, Secure data, Blockchain.

1. Introduction

The Internet has been used everywhere, in companies, organizations, governments, etc. Different people use it for various reasons. Prediction state that by 2020, machines using the Internet would increase to more than 50 billion [1]. With this increasing number of Internet users, the term Internet of Things (IoT) was introduced, which by definition, is the connection of devices to the Internet, through which they can communicate with each other and sense the environment in which they are located in, to collect and send data [2]. Common IoT applications include smart cities and industries, environmental monitoring, and health care [3]. As shown in Figure 1.

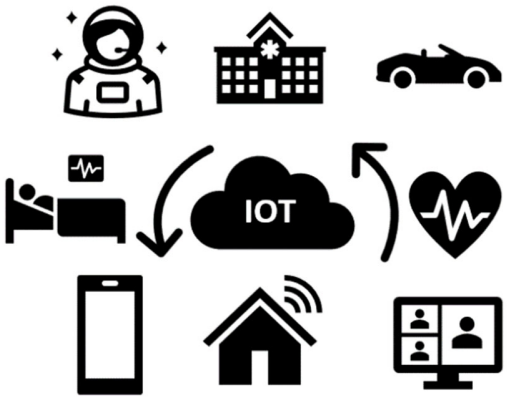

Figure 1: Internet of Medical Things

As part of the IoT, IoMTs, a.k.a. the Internet of Healthcare Things (IoHTs), became regarded for their importance in the health sector. It can be defined as a set of devices that use the Internet of Things for medical purposes, such as monitoring using sensors to record and analyze patient data [4]. This technology facilitated Remote Patient Monitoring (RPM) and the combination of the use of various smart devices (e.g., the personal digital assistant (PDA) [4] available to the patient with intelligent medical technologies. This technology generally reduces the costs associated with the medical examinations and gives medical

Manuscript received August 5, 2021
Manuscript revised August 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.8.34

healthcare professionals (HCP) a better understanding of the patient's condition [5]. As shown in figure 2.

Figure 2: Internet of Medical Things.

An application for the IOMTs was proposed within a paper [6] that aimed to develop a medical platform that would record COVID-19 patients who have mild symptoms that do not require them to attend the hospital. This data helps provide patients with the appropriate health care and follow-up on their condition while at home, which helps reduce the spread of the virus and alleviates the pressure on hospitals. An interesting example for IOMTs can be observed in wireless body area networks (WBANs), involving sensors being implanted in the patient's bodies with limited functions and storage capacity that sense the patient's biometrics and send them wirelessly to the medical professional for this patient [7] With the fast growth of the quantity of users of the Internet of medical things, there have been fears of illegally exploiting these technologies, as it was mentioned in a report by the Food and Drug Administration (FDA), for every 1,000 connected devices approximately 164 attacks are threatening them [8]. Also, what's more concerning is that the health sector is third in the industries targeted by attackers [9]. Unfortunately, there is still very little research regarding how safe the IOMTs is, and this is serious because exposing patients' data to these attacks may violate their privacy with an eavesdropping attack or threaten their lives with a Denial of Service (DoS) attack that disrupts the patient's service, which affects the rapid response of the patient and causes delays when one attempts to help [10]. Also, IoMT devices can be used as zombies that carry out severe attacks on healthcare infrastructure [11]. In this paper, we have collected many documents that emphasize how secure the IOMTs is and can be, where we begin by defining the security requirements and the meaning of security in the IoMT, after which we mention the attacks that the IoMTs are exposed to along with the proposed solutions to avoid or limit these attacks.
IoMT technology is what has facilitated Remote Patient Monitoring (RPM), which combines the use of various smart devices (e.g., personal digital assistant (PDA) available to the patient with intelligent medical technologies. This technology generally reduces the costs associated with medical examinations and gives medical healthcare professionals (HCP) a better understanding of the patient's condition. For example, the use of IOMTs was proposed in a paper to develop a medical platform that would record data for COVID-19 patients who have mild symptoms that do not require them to attend the hospital. This data helps provide appropriate health care to patients and follow up on their condition while at home, which helps reduce the spread of the virus and alleviates the pressure on hospitals.
In our paper, we shed light on recent papers regarding the security within IOMT devices from many different perspectives. In the first section, we define the term IOMT and cite a few examples. In the second section, we mention some of the security requirements of IOMT in detail, as well as some security issues it faces. The fourth section discusses several research papers that focus on privacy, confidentiality, authentication, and Detection Mechanisms for IOMT devices. Finally, we discuss the documents that we mention throughout the investigation regarding their strength, efficiency, effectiveness, and cost.

2. Security Requirements

As we all know, the rapid growth of IoT applications and implementation in many fields and industries is considered necessary in people's daily lives, making them easier spatially for those in the healthcare industry. The device collection included a handheld sensor that can be worn, actuators, and further additions that connect to communicate smoothly through the Internet [12]. However, all of these IOMT applications using the Internet come with severe security risks and threats. For this reason, IOT systems require a strong security foundation built on a comprehensive view of security for all IoT elements at all levels. With the expanding requests on quality medical services and the rising expense of care, unavoidable medical services are considered innovative answers for addressing global medical problems. Specifically, the new improvements on the Internet of Things have prompted the IoMT. Even though such minimal expense and unavoidable detection devices might change the existing responsive consideration to precaution care, the protection concerns of those sensing frameworks remain regularly neglected. As the medical devices catch and interact with delicate individual wellbeing information, the devices and their related interchanges must be exceptionally gotten to secure the client's protection. In any case, the scaled-down IoMT devices have extremely restricted calculation power, and genuinely specified security plans can be executed in such instruments. Moreover, with the inescapable utilization of IoMT machines, guaranteeing the protection of IoMT frameworks are exceptionally difficult, and the significant issues are ruining the appropriation of clinical applications of IoMT. The protection challenges, prerequisites, dangers,

and future exploration bearings in the area of IoMT are audited, giving an overall outline of the best in class draws near [63].
We consider applying specific aims to ensure that data is more secure and confidential, Integral, and Available (CIA) to IoTs to achieve high security within the communicative frameworks to benefit every user, software, service, process, and thing [13].

2.1 CIA in IoMTs

Confidentiality is considered to be one of the essential security principles. The concept of having confidential data stems from the need for security and privacy, ensuring sole accessibility to users with authorization. For this, IoT users can be classified into various categories such as a person, machine, service, internal-object (device included within the network), and an external-object (device not included within the network) [14]. Confidentiality is an integral function when dealing with users or managing processes related to user data. For example, in IOMT, patient data cannot be by unauthorized entities for the sake of privacy. Therefore, all Tags and identification information in the RFIDs are encrypted before the transition [13].

The IoT depends on how sensitive information is exchanged from one device to another. For this reason, the data need to remain untampered and unmodified by any unauthorized entity during the transition [14]. For example, in healthcare systems (IOMT), remote patient monitoring requires system integrity checks to maintain patient-sensitive information accurately. The integrity can be maintained with end-to-end security, where data traffic is controlled with the use of a firewall, error detection mechanisms, and more [14].

One of the main expectations from IoT is that each piece of information, device, and service should be excellent in terms of availability and reachability by the user when they require it on time. For
For example, healthcare monitoring systems would likely have higher availability requirements [14] [15].

2.2 Authentication and Lightweight Solutions in IoMTs

All objects within an IoT should have the ability to identify and authentication each other. However, the authentication process may not be accessible due to the involvement of numerous entities in IOTs (device, person, service, service-provider, processing-unit, etc.); some of these entities may be communicating for the first time [13] [14].

The devices involved with IoTs may have some limitations regarding their computational and power capabilities. For this unique security feature, lightweight solutions are the priority when considering the design and implementation of each protocol. Any algorithms intended to run on an IoT device would mandatorily have to ensure their compatibility with the features the machine is capable of carrying out [14].

2.3 Heterogenous IoMTs.

The nature of the IoTs is that they can connect several entities that are differently featured or capable and are exceedingly more complex, with varying different dates and release versions. Furthermore, the environment that holds these IoTs is also constantly changing (dynamics). For this reason, a protocol should be implemented to ensure that every type of device can function in all possible situations [14].

2.4 IoMTs Policies and Standards

When using IoT technology, we must ensure efficient management, protection, and transmittance of data. To achieve this, we must apply various policies and standards. Additionally, we must also consider the most critical requirement: to use a mechanism that enforces such policies on entities to apply the standers. Bringing about a procedure like this introduces confidence within users that utilize IoTs paradigms, and this causes the eventual outcome of it growing and becoming increasingly scalable [14].

2.5 Key Management Systems for IoMTs.

To achieve confidentiality in the IoT devices and sensors, there is a need for the exchange of some encryption materials between these devices, which means that there is a need to have easy to use systems to manage their keys which is capable of generating trust and distributing a key between different devices without a high capability [14].

3.Security Issues in the IoMTs.

Ensuring the security of an IoMT network is extremely important because it eliminates any potential threat that could lead to a security attack and breach the privacy of patient data. IoMT technology is referred to as the most in-demand technology within healthcare sectors. Nearly 420 million machines with a connection have been deployed worldwide in all healthcare facilities [16]. Keeping so many layers of security IoMT systems is a challenging task because these attacks harm integrated systems and threaten people's lives [17]. Modifications made to the patient's information, either through disclosure or lack thereof, may

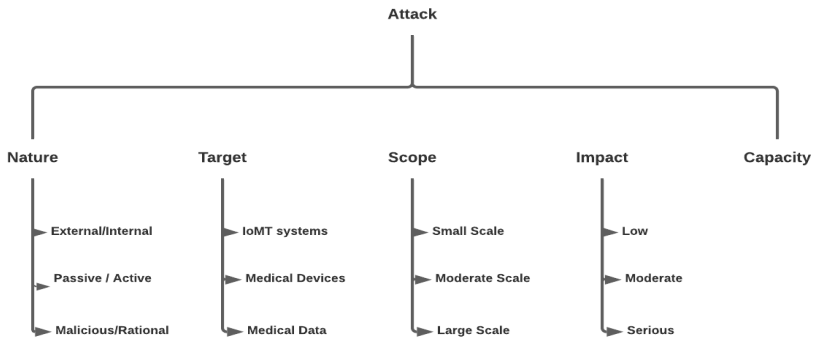

Figure 3: Categories of attacks [17]

threaten the patient's life. [18] The health care sector is not keeping pace with modern precautions for cybersecurity [19].

The authors in [17] classify the attacks into five main categories, as shown in Figure 3.

The attackers' nature: Attacks can happen in many ways; internally, externally, passively, and actively. There are instances where there may be a combination of more than one such attack to make the cyberattack more complicated [17].

1-External/internal attacker: An internal attacker can be external attackers to perform their cyberattacks with ease [17]. As for external-attacks, they are defined as a malicious intrusion that aims to access the hospital system and violate private patient data and spread or sell it to a third party with an ulterior motive using the deep dark web for actions directly related to fraudulence and this is accomplished either with the use of a worm, rootkit, or a Trojan-attack. Additionally, there are instances where the attack relies on phishing methods by submitting fraudulent PDFs or CVs. Once the download is complete, a key recorder or back door will be installed on the desired system. [17].

2-Passive and active attacks: The passive attacks attempt to remain anonymous and do nothing to avoid detection; the attacker aims for the successful interception of information being transferred from one device to another wirelessly and then collected and read for later use in a more complex cyberattack. Passive attacks may involve collaborations with external or internal attacks to gather data [17.]. As for the active attacker, he is more dangerous because he relies on intercepting patient data and then changing, deleting, or modifying it. This can be extremely dangerous and sometimes even life-threatening. For example, it can lead to the wrong medicine being prescribed to a patient or a higher dose of medication administered, which can endanger the patient's life and even lead to death [17].

3-Malicious and Rational Attackers: Malicious attackers carry out their attacks simply with the intent to disrupt the IoMT system and prove that they can do so; they possess no specific target and are not looking for any particular outcome. Rational attackers, in contrast, have a clear target that has a hazardous impact. [17].

- Target: These attacks are utilized either for terrorism or assassinations. The target can be the entire hospital or a specific patient admitted within it. The attack can be for several reasons that include ideological, religious, ethnic, or political reasons. One example would be the assassination of a public figure. In addition, the attacker may be a different nation interested in spreading terrorism or propagating racist actions [17].

- Scope: This refers to the target area, which can be large or small in size. The attackers try to expand the scope ofattacks to include larger rooms, which increases how many patients end up affected by it [17].

- Impact: How these attacks impact an area is measured by how significant the damages are, as well as the motive and extent of the same attack [17].

-Capacitance: This indicates the security needed for the prevention, mitigation, or reduction of damages resulting from the attacks [17].

3.1 The common attacks in IoMTs.

Eavesdropping attacks.

Such attacks depend on the gathering of sensitive data. They exist in two forms: active and passive eavesdropping. Passive eavesdropping scans wireless access points so that it can determine which medical device is connected to them. In contrast, in passive eavesdropping, the opponent monitors the data sent and received during transmission. Then, they use this data to gather a lot of information in an easier and faster way [20].

Data-Interception Attack.

During the execution of a man-in-the-middle attack, the opponent can intercept the data and forward it at another

time. This permits third parties to eavesdrop on Address Resolution Protocols (ARP) so that handshakes can be successfully captured. If it catches it, it uses it to enter a system and medical records without authorization and obtain encryption keys [21].

IoMT entitles interconnection of correspondence-empowered appliances and the combination of these appliances to more extensive level wellbeing networks to enhance patients' wellbeing. Notwithstanding, due to the basic idea of well-being-related frameworks, the IoMT actually faces various difficulties, especially dependability, security, and security. This paper presents a complete writing survey of late commitments zeroed in on improving the IoMT using formal philosophies given by the digital actual frameworks' population. We depict the useful use of the democratization of medical machines for the two patients and medical services suppliers. This work likewise recognizes neglected exploration bearings and expected trends to take care of unknown examination issues [64].

Message-Tampering Alteration Attacks.

Such an attack intends to tamper with the reliability of the sent messages' data to achieve his own goals, which could lead to doctors making wrong decisions that can potentially harm patients [22].

Malicious Data injection.

In this attack, a legal entity is created that can grant authentication into the system. This attack causes severe effects on the IoMT systems, leading to the end of patients' lives by creating a message containing false information and sending it to the doctors and the hospital's databases. In addition, the attacker blocks the correct and accurate message sent by a legitimate user and then injects the wrong message within the system [23].

Malicious Script Injection Attacks.

The wrong script system presents a false update, as a hacker mimics a legitimate backup server in the system. As a result, it can access the IoMT devices without authorization and also provides a tailgate [24].

Wireless Jamming.

In this attack, wireless networks are highly targeted. The attacker disables the ability of patients and hospitals to communicate with each other. Wireless networks are usually the target [25]. Continuous packets are sent from DoS attacks, disrupting all communications on every channel with any form of security. These jamming attacks either operate selectively or non-selectively. [26]. However, by shifting the frequency and moving between frequencies, the effects of this attack can be minimized, as mentioned in [27].

Flooding Attacks.

These attacks attempt to overburden the medical system and deplete its resources by flooding and injecting methods using fraudulent information and a fake request. [28].

ICMP Flooding Attacks.

It is a flood of Internet Control Message Protocols (ICMP) or Ping a DoS, which uses an ICMP echo request or a ping to attack medical devices. [29].

SYN Flood Attack or "half-open" attack.

A hacker would usually use this attack on IoMT connections that utilize a device with a higher capacity due to Transmission Control Protocols (TCPs) for communication. (i.e., a web-server/email) [30]. The primary goal of such attacks is to disable medical servers as the attacker is consuming the saved e-health care server memory to allow a connection that is not secure for a future attack.

The Black-Nurse Attack.

ICMP attacks target CPUs and firewalls with a DoS attack that prevents medical staff and patients from transporting Internet traffic within the local area network (LAN) [31].

Brute Force Attacks.

This attack searches and attempts all the possible passwords to find the correct one. They do this by breaking down every possible keyword to gain access for illegal purposes such as obtaining medical information or patient credentials. This attack includes most targeted devices and is not limited to remote medical sensors of patients [32]. [33].

Masquerading Attacks.

The striker exploits the knots node to migrate the wireless network for a variety of malicious purposes. It continuously sends false alarms on alarms that were intended for emergency medical situations. This attack can affect the availability of medical services for patients within a hospital [27]. These attacks allow the attackers to adjust the patient's recorded medical conditions, which can ultimately lead to administering the wrong medicine or excessive doses of an erroneous drug, potentially leading to the loss of life.

Replay Attacks.

The attacker can signal the system and change or make modifications to the control signals sent to other medical devices. The attackers can intercept and steal the transmitted information as he redirects it to another location. This can cause physical damage to the medical systems [34]. System connections are initially recorded and then 'replayed' later in the receiving device [35]. The hacker would have the ability to leak, steal, disclose private patient information, access specific medical systems without authorization, and obtain a high privilege within them. [36].

Dictionary Attacks.

This attack occurs when accessing medical systems without authorization [37] when the security measures are not stringent enough for the IoT device. These attacks rely on a group of dictionary words to try to guess passwords. This type of attack is comprehensive in terms of time and resources, ranging from minutes, hours to even days. [38].

In this attack, they rely on a group of numbers known as the Personal Identification Number (PIN).

Birthday Attacks.

Often users rely on weak hashes, as two passwords may contain the same hash. The hacker exploits this weakness and accesses the medical systems without authorization. [39]. The best solution to protect the systems from such attacks is to use secure hash algorithm mechanisms (SHA-512 and SHA-3).

Worms.

This is the most dangerous and destructive form of malware present within Things [40]. They can self-reproduce without human intervention via a connected device and take advantage of the device's vulnerabilities. It affects all devices and data security services (confidentiality, safety, and availability), which leads to data loss and even sometimes affects patients' health and even be the reason for the loss of human lives. They are programmed to affect specific industrial control systems [41]. Recently, a few "dubbed" malicious Internet worms targeting a network were introduced in one of the articles [42]. A worm can be executed and utilized as an attack on an IoMTs device to collect and steal information to destroy a specific device. Suppose an attacker installs insecure devices in an IoMT. In that case, he can put the entire medical system at risk by infecting them with worms, as they automatically spread themselves in the whole system when exploiting vulnerabilities in the system. Worms work in combination with different harmful species like botnets or ransomware, which helps them spread across the entire IoMTs network. [43] .

Table. 1 summarizes the different types of malware that can be found.

4. Related Work

4.1 Privacy and Confidentiality of IoMTs.

The authors of the paper [44] refer to security concerns related to the security issues of privacy of user data for the IoMTs in the dynamic, distributed, heterogeneous and interconnected network of widespread IoT devices, and they made clear that perhaps at present, the privacy of users does not seem that important. However, its importance is expected to expand in the future due to the rapidly increasing amounts of data from a higher user population, which makes preserving the privacy of the individual a significant issue that must be urgently addressed. The researchers suggested that IoHT devices should be independent, with the ability to identify the risks they face and deal with them through a subjective, foundational method. Additionally, many risks can be avoided if users' identities are specified based on the device they use.

The paper [45] discusses five data-related issues regarding having a secure, private, robust, spacious network that lacks integrity. The researchers suggested two encryption methods that may be able to combat any such concerns successfully. Attribute-based Encryptions (ABCs) and Advanced-Encryption Standards (AES) with Provable-Data Possessions (PDPs) are the methods used to promote data integrity. The process begins by using both asymmetric encryption and the AES to encrypt data in its various forms. After that, the AES encryption key is generated. The security level of AES is determined according to the requirements specified by the algorithm used. It is often within three levels, a minimum of 128 bits, an average limit of 192 bits, and an upper limit that does not exceed 256 bits. Then the AES encryption key is used for ABE encryption, after which CP-ABE (Ciphertext-Policy Attribute-Based

Table 1: summary the different types of malware [17]

Malware	Detection Mechanisms	Possible cause	Associate Threats
Botnet	An antimalware, pen-testing, intrusion detection system (IDS)	Exploits IoMT logical vulnerabilities	One or more security requirements (e.g., confidentiality, integrity, authentication, and availability)
Worm and Viruses	Antivirus, antimalware, pen-testing, IDS	Failure of security networks	One or more security requirements (e.g., confidentiality, integrity, authentication, and availability)
Spyware	Keeping the software and operating systems up-to-date and using Antivirus	It needs a host	One or more security requirements (e.g., confidentiality, integrity, authentication, availability, and especially privacy.)
Remote Access Trojan	Continuous hardware update, IDS use	It is installed by downloading a program or a software update then it hidden in the device	One or more security requirements (e.g., confidentiality, integrity, authentication, and availability)
Rootkit	Suitable configuration for System and management, authentication, IDS, and patch.	Exploits kernel or space inside the application has root characteristics.	Authentication
Ransomware	Awareness, Antivirus, and keep away from using private information.	Use weak passwords, ransomware extortionate	One or more security requirements (e.g., confidentiality, integrity, authentication and availability, and privacy.)

Encryption) is used to compare AES security levels. And finally, both the AES and the AES keys related to CP-ABE are transmitted securely. After which decryption takes place, the AES keys using the ABE Key, which is then later used to decrypt the data. Ensuring the integrity of both AES and AEB required the use of PDP. This allows the server data to be verified, and the method has proven to be especially effective ever since the COVID-19 virus and the pandemic began as shown in figure 4.

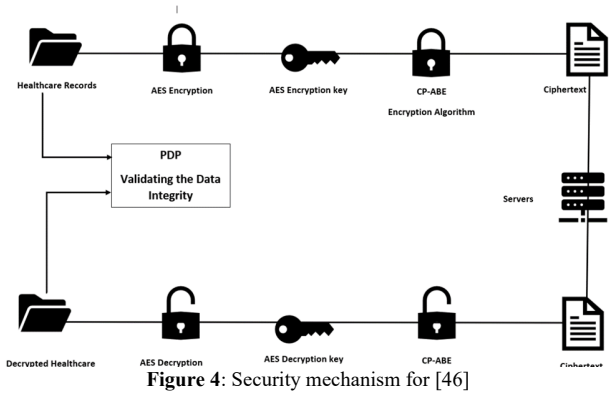

Figure 4: Security mechanism for [46]

Blockchain technology has contributed to strengthening many aspects of IoMT, as mentioned in the paper [46], where it focused on five elements, namely: finding the origin of the epidemic, remote health care, social distancing, the intelligent hospital, and the source of data for people with the virus. Privacy is a hindrance to IoMT expansion and how blockchain technology has reduced the complexity and heterogeneity of IoMT devices and has been called BlockchaIn-enabled IoMT. Blockchain can be addressed as something advantageous because they help manage privacy and security issues via a digital signature and an asymmetric encryption/decryption method and masking blockchain addresses that contain patient data. The authors [47] proposed a classification that divides the risks to privacy and security (P&S) in IoT based on the five layers:

- Perception Layer: This layer is responsible for collecting patient data such as measuring the pulse rate by using various sensors after receiving the network layer.
- Network Layers: These layers are responsible for directing what comes from the data to the appropriate path using various technologies such as Wi-Fi or radio waves
- Middleware: This layer is a filter for the Perception layer, and it is also responsible for performing access control.
- Application Layer: This layer acts as an intermediary between the user and the IoMT devices.
- Business Layer: This is between two parties that attempt to keep their identities anonymous from each other to achieve security and efficiency simultaneously.

In this work [48], the authors expressed concern about revealing data stored in IoMT devices that invaded users' privacy while simultaneously ensuring that the data source was a reliable IoMT device. They did this by proposing an approach that would be effective in preserving privacy. Their idea was to merge both elliptic curve digital signature algorithm (ECDSA) and (DS) dual signature to exchange data on breaches (Spoof, Tamper, Repudiate, Disclose data, DoS, Elevate Privilege) as a base for identifying potential risks. Both Wi-Fi Dongle and Raspberry Pi were used as a gateway to set up IOHC devices so that these devices could access the Internet without affecting the network as a whole. Access to the database is done using Echo Dot. This is data that Raspberry Pi hosts using two IOMT devices (glucose monitor and temperature monitor) in addition to the AD8232 ECG Module and key. This model was built to assess potential risks and arrived at the necessity to codify the exposed data for different parties and give the patient the authority to accept or reject the prescription and send their responses to the doctor, in addition to providing specific powers to the manufacturers to update the system without getting access to any of the users' data.

For this paper [49], the researchers developed a system that would protect patients' privacy from unlawful violations used for criminal acts that can potentially result in many damages, including losing a patient's life. In addition, the authors use STRIDE to perform the commercial management of IOMT content. The classification of the various attacks must also be looked into so that that information will be a rich reference for anyone who wants to know what attacks IoMT devices are vulnerable to.

4.2 Authentication Protocols in IoMTs.

To achieve security and solve problems related to the RFID in the IoMT, the authors of this research [50] proposed Novel Lightweight Authentication Schemes for RFID that requires additional Security Demands such as Untraceability, Forward secrecy, Resilience to impersonation attacks, Resistance to desynchronization attacks, as well authenticated access, and to achieve that, they initially display the results obtained by analyzing Fan et al.'s scheme security. The analysis shows that the scheme is weak against multiple attacks such as impersonation attacks. This weakness is then combatted by introducing the RFID scheme that also preserves the main security requirements. As a result, the proposal schemes are lightweight and conforms to the EPC C1G2 standard. For this study, [51] the authors introduced a newer design for the blockchain-enabled authentication key agreement protocol for IoMT environments (BAKMP-IoMT); this new approach allows keys to be securely managed for the Implantable Medical Device (IMD), personal-servers (PS), and any server on the cloud, a.k.a., Cloud Servers (CS). In addition, BAKMP-IoMT includes features such as the

ability to use a single-directional cryptographic hash function and a bitwise XOR operation.

There are eight phases involved when using this method; First of all, the pre-deployment phase is performed, which involves the registrations of all entities (IMD, PS, CS). This is done using a Trusted Authority (TA). Secondly, the critical management phase focuses on securing the communication between the IMD to PS and PS to CS to introduce a secret set of pairwise keys for secure transmission. The third phase is the user registration phase that mandates high security when registering with trusted authorities (TAs) to access the data in the IMD stored in the Blockchain. The final few steps include logging in, agreeing and authenticating keys, constructing and adding Blockchain, updating passwords and biometrics, and adding dynamic IMDs. This approach allows keys to be managed securely between different entities and provides secure access to the cloud to only authorized users; the authors proved that the design is resilient against multiple adversarial attacks, including replay attacks, man-in-the-middle (MIMA) attacks, the impersonating attack, and others. Through the use of AVISPA tools with formal and informal analyses and BAKMP-IOMT, the method proved itself to be one among the more relevant schemes discussed previously as it was secure and functional, and the fact that it utilizes the minimum amount of communication and costs for the same in terms of authentication. Its impact on performance is also significantly reduced.

This paper [52] introduces a cryptographic access control protocol that combatted the conventional access control scheme. The proposed method attempts to ensure that a user is authenticated with high security using key agreement schemes with the help of the WBAN systems depending on the Diffie-Hellman key exchanges. With this secure scheme, they establish reliable channels in which the registration process for the system members can take place. The authors believed that the proposed method could handle the challenges that were faced by the IoMT systems. Another paper [53] proposed a 3-factor authentication system that had a time limit and had anonymous users within a 5G-based wireless sensory network; the use of these three factors (biometric detection, passwords, and smart-cards) enhances and secures the communication space between the communication entity and provides a fast authentication which in turns helps to achieve faster communication at the same time. In addition, it helps hide the user's identity. The proposal protocol was designed to have multiple servers that allow the usage of one passcode to utilize several features from every server, thereby reducing the load on the networks and the cost of the database. When two users desire to communicate, they must register with a trusted third party and then compute their shared session key securely and share it through public channels. They will be authenticated only after initializing, reporting, and logging in. This happens with the definition of an identity partially as a subset of the users' or devices' IDs so that their data can be preserved and kept private while at the same time still being able to confirm who they are. This is followed up with an example of applications for these frameworks using Distributed Capability-Based Access Control. Each attribute is saved using evidence that will then be utilized when authorizing users using XACML to produce a capability token that permits a user to use a feature within the network or device [54].

4.3 Detection Mechanisms for IoMTs Networks.

Wazid et al. [55] discuss the different types of malware attacks, the structure of the IoT/IoMT systems, and their applications. They also attempted to classify the security protocols implemented in the IoT environment. A comparative study was conducted on the current schemes used to detect and prevent malware in the IoT environment. They also focused on future research and its challenges, and various aspects of malware detection in the IoT / IoMT environment. To protect against Sybil attacks on the IoMTs, the authors in [56] proposed a trust management mechanism based on Fuzzy (FTM-IoMT). This mechanism enables users of e-health systems to manage their trust when using Internet infrastructure. This mechanism is an intelligent mechanism that helps identify unreliable nodes in the system or Sybil. It also allows IoMT nodes to ignore the Sybil nodes and collect reliable information from trusted neighboring nodes. Fuzzy logical manipulation is used to assess the trust value in terms of its compatibility, viability, and node integrity. Also, (FTM-IoMT) provides a dual-check evaluation based on fuzzy filter and fuzzy logic processing. This mechanism uses the First In First Out (FIFO) function to identify priority contract orders. Then the server provides services to the node following the experience of the server when encountering such transactions when the database was updated.

In FTM-IoMT, the reliability of IoMT nodes is evaluated using fuzzy logic processing. When a request is received from a node, the server considers the node's trust through fuzzy logic processing, and ambiguous rules are applied to the node before it is sent. Then the server gets the final value of the belief in the node, and based on that value, the server either decides to provide the service or ignores the node and assigns the specific value to fight the malicious nodes. In this mechanism, conformance and integrity attributes are used as confidence parameters to evaluate node confidence. An analysis of these mechanisms was performed in different classes, including homogeneous and heterogeneous nodes. The proposed mechanism showed promising results compared to modern methods.

For the timely detection of complex malware, the authors in [57] introduced a hybrid DL-based IoMT framework that uses SDN that leverages the convolutional neural networks (CNNs) and the long-term deep neural

network memory. The presented framework was compared with hybrid architecture based on the algorithms metering and DL. The proposed tire has proven its worth in terms of test efficiency and detection accuracy.

The authors in [58] provide web-based IoMT Security Assessment Frameworks (IoMT-SAF) and this scenario-based framework to introduce the necessary IoMT security measures, deterrence, and protection assessment IoMTs. IoMTs-SAF advises choosing a compatible solution with the users' security goals that helps the decision-making process. The novelty of IoMTs-SAF is entirely due to its scalability, detail, and ability to begin adapting to a newer user and is compatible with medical, technical, and other standards. To enhance the rapid and safe recognition of subtypes of leukemia, the authors have introduced an Internet Medical Framework (IoMT) where [60] they used cloud computing in which network resources are linked to clinical tools. The proposed framework saves physicians and patients time and effort as it coordinates the communication of a healthcare professional when attempting to diagnose and treat their patients. DenseNet-121 and ResNet-34 were used in the presented framework to identify the subtypes of leukemia. An IoT supported the uploading of microscopic images of blood smears to the leukemia cloud. A diagnosis is then made using the DenseNet-121 or ResNet-34 models. After a patient is diagnosed, this is then communicated to the system owned by the doctor's computer. He will provide the necessary care based on the test report by IoMT. In this study, information on two widely available groups for leukemia ALL-IDB and ASH image bank was collected. It has been noted that diagnostics using ResNet-34 and DenseNet-121 is very effective and can replace all previous methods that existed. The provided framework also helps patients that are suffering during epidemics such as COVID-19.

Because of the urgent need for new security mechanisms to keep the IoMT network secure, in this paper [60], a basis has been provided to organize, classify and develop appropriate security measures to protect against internal and external threats to IoMT networks are vulnerable. It also provides a classification system for the terminal network's internal and external security threats that target the main security objectives. The authors in [61] provide a framework based on IoMT's fog cloud architecture that was proposed for the detection of cyber-attacks, the (SaaS) service is used in the fog, and the infrastructure and the (IaaS) service is used in the cloud. It also uses the ToN-IoT framework, where realistic data is collected from a large-scale or heterogeneous IoT network.

5. Discussion.

After reviewing many research papers related to confidentiality and privacy issues, it was noted that the privacy aspect of an IoMT device user is highly vulnerable to violation and illegal exploitation by parties benefiting from this data. It was also pointed out that negligence in taking the privacy issue seriously and considering it an additional feature even though this data doubles its value over time. In the worst cases, its violation may endanger the patient's life. One of the researchers suggested that IoMT devices be independent devices that discover, identify and prevent the risks they face. This is, of course, a suggestion worth noting and has the potential to reduce attacks significantly, but it may need development and improvement to achieve this goal. Another idea that was put forward was to use both AES, ABE, and PDP as encryption methods that prevent unauthorized persons from accessing or exploiting any stored data. Still, this method needs to be implemented in different circumstances to ensure its effectiveness. The authors also mentioned that it could be developed and used as artificial intelligence for encryption, making it more efficient and safer in the future. Also, using new encryption technologies such as ECDSA for encryption and signature verification is more powerful. It counteracts modern attacks, although it is slower and more expensive than old technologies such as RSA. The most common challenge that IoMTs faced is each device regarding its complexity and inconsistency. Hence, one of the researchers suggested a way to overcome them through blockchain technology used to encrypt and hide data for IoMT users. Still, the challenges that this technology faces, such as price and scalability, must also be considered. Classifying layers facilitate the process of communication and make it easier to address security and privacy challenges because, after understanding each layer on an individual basis and realizing how it was adversely affected during the attack, we can know what we need to do to maintain the security of that specific part or layer separately. Finally, it is essential to provide IoMT devices that preserve user privacy in any environment they are placed in, and this is something that interested parties (s.a., developers and officials) should take care of and try to start developments where they can set clear policies that preserve users' privacy. Finally, balancing costs to keep the network secure, functional, and easy to use is a requirement that increases the efficiency of IoMT devices. Several methods are chosen to achieve this authentication that ultimately aims to secure the IoMT environment. For example, several research papers discuss authentication and its distinct protocols using lightweight encryption algorithms. It consumes fewer resources during computation, is more efficient than traditional cryptographic algorithms, and is also suitable for devices with limited computing power.

When the methods were validated based on their applications within all of the literature mentioned, they focused on achieving the various security requirements. They concentrate on verifying the safety and integrity of those technologies proposed in multiple ways. For example, in some papers, this test is conducted using specific tools or specific techniques that help determine various aspects

regarding the effectiveness of a proposed scheme. For example, these tests can be performed using a GNY Logic Analysis (gong - Needham - Yahalom) or VISPA tools that implement the specified simulation protocol using HLPSL.

Other papers focus on the process of comparing proposals and past diagrams to find differences in terms of their fulfillment of safety, performance, cost requirements, and their Resistance to security attacks. For example, in the new lightweight validation scheme for RFID based healthcare systems proposal, the authors make comparisons with other existing plots using concepts introduced by Fan et al. As a result of this comparison, it was found that complete confidentiality cannot be guaranteed, as it is fragile against impersonation attacks. However, the proposed scheme has been quite successful in overcoming such security weaknesses.

To achieve detection mechanisms in IoMTs, several recent research papers presented in 2019 and 2021 have been studied that looked at reference [56] nodes. It was noted that the energy consumption by FTM-IoMT is lower than that of GroupTrust, RobustTrust, and SGSQoT, and the time taken by the FTM-IoMT mechanism to calculate trust values was less than that of GroupTrust. One of the features we liked about FTM-IoMT is that it detects more malicious nodes than RMB-TC and FR-Trust due to its use of vague evaluation logic. Also, the proposed mechanism has greater production efficiency compared to other schemes. Therefore, FTM-IoMT is based on fuzzy logic, as it is considered the best candidate used to train intelligent systems and help them make decisions.

About [57], the proposed technology outperformed DL-based architectures as well as DNN-GRU and LSTM-GRU. We were impressed that SDN networks silenced the proposed mechanism to prevent the additional burdening of the core resources of IoMT. The recommended agencies outperform due to their complexity, computation, and disclosure. To see the result frankly and unbiased, a 10-fold validation was performed, in which [58] IoMT-SAF was able to successfully identify most of the security issues and was also able to work with the distinct scenarios of IoMT, which was impressive considering that the IoMT-SAF has the scalability and compatibility that is different for each user. However, we found several drawbacks to using IoMT-SAF, such as using a wide range of evaluation features causing the complexity to define and lengthen security profiles. In addition, it is not easy for novice users such as medical staff and patients to understand the features of the evaluation as they lack technical and security awareness. In [59], the proposed model proved its efficiency, as a comparison was made between the proposed model with previously used methods; GA with SVM and CNN. That is, GA uses SVM to identify AM L and ALL samples and each healthy sample, and CNN identifies the leukemia subtypes. The use of ResNet-34 and DenseNet-121 in the proposed model beats any scheme that existed, including GA with SVM and CNN. Studies have shown the accuracy of GA with CNN to be 81.74%, SVM has 99.50%, ResNet-34 is accurate to up to 99.56 percent, and DenseNet-121 is valid up to 99.91 percent, so DenseNet-121 outperforms all the other approaches. We like the proposed model in [61] because it saves time and effort to detect leukemia and its subtypes compared to machine learning techniques. We enjoyed the proposed framework because it achieves an accuracy rate of 96.35% and a detection rate of 99.98%, proving that the proposed framework is excellent and reduces the false alarm rate to 5.59%.

6. Conclusion.

The Internet of Things is one of the terms that have become associated with us in the current era, and its applications and uses in various fields and sectors have varied. One of its most important applications is the IoMTs, which is defined as devices connected through the network and used to monitor the patient or user remotely using sensors that collect the data, store it and send it to the party health concerned with this data. However, with all the advantages provided by IoMT devices, the security aspect therein is highly vulnerable to violations; for this purpose, our paper focused on presenting a comprehensive study of published and recent research on the safety of IOMT devices and the challenges they face in addition to offering several solutions to confront them, also to discussing and comparing these methods in terms of how efficient, effective and costly they were. In the future, we hope to develop strategies and safety mechanisms and conduct more research and investigations regarding the security of IMOT.

References

[1] Ghorbani, H. R., & Ahmadzadegan, M. H. (2017, November). Security challenges in the Internet of things: a survey. In 2017 IEEE Conference on Wireless Sensors (ICWiSe) (pp. 1-6). IEEE.

[2] Fizza, K., Banerjee, A., Mitra, K., Jayaraman, P. P., Ranjan, R., Patel, P., & Georgakopoulos, D. (2021). QoE in IoT: a vision, survey, and future directions. Discover the Internet of Things, 1(1), 1-14.

[3] Shanthamallu, U. S., Spanias, A., Tepedelenlioglu, C., & Stanley, M. (2017, August). A brief survey of machine learning methods and their sensor and IoT applications. In 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA) (pp. 1-8). IEEE.

[4] Ahmed, G., Mehmood, D., Shahzad, K., & Malick, R. A. S. (2021). An efficient routing protocol for the Internet of medical things focusing on hot spot node problems. International Journal of Distributed Sensor Networks, 17(2), 1550147721991706.

[5] Harvey, P., Toutsop, O., Kornegay, K., Alale, E., & Reaves, D. (2020, December). Security and Privacy of Medical Internet of Things Devices for Smart Homes. In 2020 7th

International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 1-6). IEEE.

[6] Yang, T., Gentile, M., Shen, C. F., & Cheng, C. M. (2020). Combining point-of-care diagnostics and the Internet of medical things (IoMT) to combat the COVID-19 pandemic.

[7] Kumar, M., & Chand, S. (2020). A lightweight cloud-assisted identity-based anonymous authentication and critical agreement body area network. IEEE Systems Journal.

[8] Food and Drug Administration, HHS, "Design considerations and premarket submission recommendations for interoperable medical devices," Sept. 2017.

[9] Karmakar, K. K., Varadharajan, V., Tupakula, U., Nepal, S., & Thapa, C. (2020, June). Towards a Security Enhanced Virtualised Network Infrastructure for Internet of Medical Things (IoMT). In 2020 6th IEEE Conference on Network Softwarization (NetSoft) (pp. 257-261). IEEE.

[10] Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the Internet of medical things enabled healthcare systems: A survey. IEEE Access, 7, 183339-183355.

[11] Angrishi, K. (2017). Turning Internet of things (IoT) into the Internet of vulnerabilities (iov): IoT botnets. arXiv preprint arXiv:1702.03681.

[12] X. Huang and S. Nazir, "Evaluating Security of Internet of Medical Things Using the" Security & Communication Networks, p. 15, 1 September 2020.

[13] Nazir, A., Sholla, S., & Bashir, A. (2019). Internet of Things Security: Issues, Challenges, and Countermeasures. International Journal of Network and Technology, 7(3).

[14] T. Y. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges, and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE.

[15] Puat, H. A. M., & Abd Rahman, N. A. (2020, December). IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. In Journal of Physics: Conference Series (Vol. 1712, No. 1, p. 012009). IOP Publishing.].

[16] Yaacoub J.-P.A., Noura M., Noura H.N., Salman O., Yaacoub E. Securing internet of medical things systems: limitations, issues, and recommendations. Future Generation. Comput. Syst. 2020;105:581–606

[17] Javdani, H.; Kashanian, H. Internet of things in medical applications with a service-oriented and security approach: A survey. Health Technol. 2018, 8, 39–50.][Altawy, R.; Youssef, A.M. Security Tradeoffs in Cyber-Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access 2016, 4, 959–979.

[18] Singh, J., & Abd Rahman, N. A. (2020). IoMT: A review of Open APS System Security for Type 1Diabetes Mellitus. Int J Cur Res Rev| Vol, 12(17), 93.

[19] David D Coleman and David A Westcott. Cwna: certified wireless network administrator official study guide: exam Pw0-105. John Wiley & Sons, 2012.

[20] Daojing He, Sammy Chan, and Mohsen Guizani. Drone-assisted public safety networks: The security aspect. IEEE Communications Magazine, 55(8):218–223, 2017

[21] Chun-Wei Yang, Tzonelih Hwang, and Tzu-Han Lin. Modification attack on qsdc with authentication and the improvement. International Journal of Theoretical Physics, 52(7):2230–2234, 2013.

[22] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1):13, 2011.

[23] MdAshfaqur Rahmanand Hamed Mohsenian-Rad.False data injection attacks with incomplete information against intelligent power grids. In Global Communications Conference (GLOBECOM), 2012 IEEE, pages 3153–3158. Citeseer, 2012.

[24] Satish Vadlamani, Burak Eksioglu, Hugh Medal, and Apurba Nandi. Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics, 172:76–94, 2016.

[25] Alejandro Proano and Loukas Lazos. Selective jamming attacks in wireless networks. In 2010 IEEE International Conference on Communications pages 1–6. IEEE, 2010.

[26] Kanika Grover, Alvin Lim, and Qing Yang. Jamming and anti-jamming techniques in wireless networks: a survey. International Journal of Ad Hoc and Ubiquitous Computing, 17(4):197–215, 2014.

[27] Zubair A Baig and Abdul-Raoof Amoudi. An analysis of clever grid attacks and countermeasures. Journal of Communications, 8(8):473– 479, 2013.

[28] Harshita Harshita. Detection and prevention of ICMP flood DDoS attack. International Journal of New Technology and Research, 3(3), 2017.

[29] Mitko Bogdanoski, Tomislav Suminoski, and Aleksandar Risteski. Analysis of the syn flood dos attack. International Journal of Computer Network and Information Security (IJCNIS), 5(8):1–11, 2013.

[30] Yuquan Shan, George Kesidis, Daniel Fleck, and Angelos Stavrou. Preliminary study of fission defenses against low-volume dos attacks on proxied multiserver systems. In 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), pages 67–74. IEEE, 2017.

[31] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. Cy- cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(4):853–865, 2010.

[32] Emma McMahon, Ryan Williams, Malaka El, Sagar Samtani, Mark Patton, and Hsinchun Chen. Assessing medical device vulnerabilities on the Internet of things. In 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), pages 176–178. IEEE, 2017.

[33] Pardeep Kumar and Hoon-Jae Lee. Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1):55–91, 2012.
[34] Sarah Spiekermann. Ethical IT innovation: A value-based system design approach. Auerbach Publications, 2015.].
[35] Lukas Grunwald. New attacks against RFID systems. GmbH Germany, 2006.
[36] Junghyun Nam, Juryon Paik, H-K Kang, Ung Mo Kim, and Dongho Won. An offline dictionary attack on a simple three-party key exchange protocol. IEEE Communications Letters, 13(3):205–207, 2009.
[37] Jung-Sik Cho, Sang-Soo Yeo, and Sung Kwon Kim. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer communications, 34(3):391–397, 201
[38] Mihir Bellare and Tadayoshi Kohno. Hash function balance and its impact on birthday attacks. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 401–418. Springer, 2004
[39] J. Deogirikar and A. Vidhate. Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), pages 32–37, 2017.
[40] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. Stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6):29, 2011.
[41] Sam Edwards and Ioannis Profetis. Hajime: Analysis of a decentralized internet worm for IoT devices. Rapidity Networks, 16, 2016.
[42] Evan Cooke, Farnam Jahanian, and Danny McPherson. The zombie roundup: Understanding, detecting, and disrupting botnets. SRUTI, 5:6– 6, 2005
[45] Solangi, Z. A., Solangi, Y. A., Chandio, S., bin Hamzah, M. S., & Shah, A. (2018, May). The future of data privacy and security concerns in Internet of Things. In 2018 IEEE International Conference on Innovative Research and Development (ICIRD)(pp. 1-4). IEEE.
[46] Rathnayake, R. M. P. H. K., Karunarathne, M. S., Nafi, N. S., & Gregory, M. A. (2018, November). Cloud enabled solution for privacy concerns in internet of medical things. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-4). IEEE.
[47] Dai, H. N., Imran, M., & Haider, N. (2020). Blockchain-enabled Internet of Medical Things to Combat COVID-19. IEEE Internet of Things Magazine, 3(3), 52-57.
[48] A lsubaei, F., Abuhussein, A., & Shiva, S. (2017, October). Security and privacy in the internet of medical things: taxonomy and risk assessment. In 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops) (pp. 112-120). IEEE.
[49] Cano, M. D., & Cañavate-Sanchez, A. (2020). Preserving data privacy in the internet of medical things using dual signature ECDSA. Security and Communication Networks, 2020.
[50] Harvey, P., Toutsop, O., Kornegay, K., Alale, E., & Reaves, D. (2020, December). Security and Privacy of Medical Internet of Things Devices for Smart Homes. In 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 1-6). IEEE.
[51] Zhu, F., Li, P., Xu, H., & Wang, R. (2020). A Novel Lightweight Authentication Scheme for RFID-Based Healthcare Systems. Sensors, 20(17), 4846.
[52] Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J., & Park, Y. (2020). BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for Internet of medical things deployment. IEEE Access, 8, 95956-95977.
[53] Yan, X., Geng, T., & Ding, H. (2014). Efficient cryptographic access control protocol for sensitive data management. Journal of Computers, 9(1), 222-228
[54] Wong, A. M. K., Hsu, C. L., Le, T. V., Hsieh, M. C., & Lin, T. W. (2020). Three-Factor Fast Authentication Scheme with Time Bound and User Anonymity for Multi-Server E-Health Systems in 5G-Based Wireless Sensor Networks. Sensors, 20(9), 2511.
[55] Chen, F., Luo, Y., Zhang, J., Zhu, J., Zhang, Z., Zhao, C., & Wang, T. (2018). An infrastructure framework for privacy protection of community medical internet of things. World Wide Web, 21(1), 33-57.
[56] Wazid, M., Das, A. K., Rodrigues, J. J., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: analysis and research challenges. IEEE Access, 7, 182459-182476
[57] Wazid, M., Das, A. K., Rodrigues, J. J., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: analysis and research challenges. IEEE Access, 7, 182459-182476
[58] Liaqat, S., Akhunzada, A., Shaikh, F. S., Giannetsos, A., & Jan, M. A. (2020). SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT). Computer Communications, 160, 697-705.]
[59] Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. Internet of Things, 8, 100123.]
[60] Bibi, N., Sikandar, M., Ud Din, I., Almogren, A., & Ali, S. (2020). IoMT-Based Automated Detection and Classification of Leukemia Using Deep Learning. Journal of healthcare engineering, 2020
[61] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2020). A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies, e4049

Ghada Aljumaie received the B.Sc. degree in Computer Engineering from Taif University, Saudi Arabia, in 2018. Currently, she is a graduate student at Taif University. She is doing her master's degree in cybersecurity studies. Her research interests include Cyber Security, Computer Networking .and the Internet of Things.

Ghada Alzeer received the B.Sc. degree in Computer Engineering from Taif University, Saudi Arabia, in 2018. Currently, she is a graduate student at Taif University. She is doing her master's degree in cybersecurity studies.. Her research interests include the Internet of Things, Cyber Security and Wireless Sensor Networks.

.

Reham Alghamdi received the B.Sc. degree in Computer Science from Taif University, Saudi Arabia, in 2015. Currently, she is a graduate student at Taif University. She is doing her master's degree in cybersecurity studies. Her research interests include System and social media security, Artificial Intelligence.

Hatim Alsuwat is an assistant professor of Computer Science in the College of Computers and Information Systems at Umm Al-Qura University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Information Security, Cryptography, Model Drift, and Secure Database Systems.

Emad Alsuwat is an assistant professor of computer science in the College of Computers and Information Technology at Taif University. He received his Ph.D. from the department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include Probabilistic Graphical Models (esp. Bayesian Networks), Artificial Intelligence, Information Security, and Secure Database Systems.