A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends

Yusuf Perwej, Nikhat Akhtar, Neha Kulshrestha,, Pavan Mishra

JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends

[1]Dr. Yusuf Perwej, [2]Dr. Nikhat Akhtar, [3]Neha kulshrestha, [4]Pavan Mishra

[1]Professor, Department of Computer Science & Engineering, Ambalika Institute of Management and Technology, Lucknow, India
[2]Associate Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India
[3]Assistant Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India
[4]Assistant Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India

Abstract **—** Healthcare system is rapidly transitioning from a traditional health-center and specialist-focused model to a more scattered, patient-centric model. Medical Internet of Things (MIoT) provides machine-to-machine contact and real-time intervention solutions, which in the near future will drastically revolutionize healthcare delivery, affordability, and reliability. The Medical Internet of Things (MIoT) is a new technology that aims to improve patient quality of life by allowing individualized e-health services irrespective of time or place. The Medical Internet of Things (MIoT), often known as healthcare IoT, is a network of medical devices and applications. MIoT applications are intimately linked to sensitive healthcare services, particularly because they manage sensitive patient information such as names, health records, addresses, and health problems. The key problem in the MIoT area is to protect the confidentiality and privacy of patients without compromising security. The security and privacy of data acquired from MIoT devices, either while transmission to the cloud or while kept in the cloud, are key unsolved challenges, as this data is heavy, sensitive, and require a high level of security. We examine present security and privacy challenges, as well as security and privacy needs connected to data flow in the MIoT, as well as technical shortcomings and research issues for future work, in this paper. Finally, we can state that the growing adoption of the MIoT in recent years has brought enormous benefits to both medical organizations and their patients.

Index Terms — Medical Internet of Things (MIoT), Security, Cybercrime, Privacy, Internet of Thins (IoT), Wearable Sensors, Healthcare, Cyber Security.

1. Introduction

The Internet of Things (IoT) has emerged as one of the most promising technologies in the previous decade, attracting the attention of various academic studies and industry [1]. The Internet of Things (IoT) system has a complicated design, with several components interacting with one another to provide a variety of solutions for the end user. This is a multi-tiered system that allows for real-time data collection, device connectivity, data transfers, and analytics to control end-user applications [2]. Cyber physical systems are critical components of any IoT architecture because they combine human interaction with computer-based structures and allow for data-driven decision-making. The Internet of Things (IoT) creates a connected ecosystem comprised of cyber physical systems that integrates human participation with computer-based systems and allows for data-driven

decision-making. Smart grids, smart homes, intelligent logistics, and smart communities are examples of IoT technologies that are reinforced by sensor, actuator, and communication protocol networks. Through the combination of data analytics and sensors implanted in machines, IoT provides a variety of real-time solutions. In the field of healthcare, the Internet of Things (IoT) [3] plays a critical role in a variety of applications. Clinical care, remote

monitoring, and situational awareness are the three steps of this criterion. Researchers are increasingly interested in improving the health sector in response to human needs by [4] digitizing and decentralizing healthcare institutions and providing continuous and remote medical monitoring, thanks to the rapid development of wearable/implantable sensors and wireless communication. A network of linked devices that perceive crucial data in real time is referred to as the Medical Internet of Things (MIoT), a healthcare application of IoT technology [5].

Medical Internet of Things (MIoT), which is crucial in decreasing healthcare expenses, providing fast medical responses, and improving the quality of medical treatment, is becoming increasingly significant in the healthcare business to create the safety and health system in human civilization [6]. MIoT is a novel e-healthcare technology that uses small wearable devices or implantable sensors to collect important bodily metrics and monitor pathological aspects of patients. Many healthcare providers [7] are implementing MIoT apps to improve treatments, manage diseases, decrease errors, improve patient experience, manage medications, and cut costs [8]. Increased patient participation in [9] decision-making will also improve healthcare service compliance. Artificial intelligence (AI) [10], machine learning, the Medical Internet of Things (MIoT), and Big Data (11] analytics have all aided in establishing the form of the digital healthcare business [12]. As a result, technology adoption will accelerate in the future years, propelling the market to a global value of $ 254.2 billion by 2026.

Furthermore, MIoT systems include applications for operating, monitoring, and controlling. Application risks, such as authentication and authorization breaches [13], as well as the application's general security and availability, become a worry [14]. However, because of the wide variety of medical devices in the MIoT, hostile devices may be able to modify and tangle the codes of healthcare apps. Patient-related data security and privacy [15] are two essential principles. Data [16] security refers to how data is stored and transported securely to ensure its integrity, validity, and authenticity, while data privacy refers to how data can only be accessed by those who are authorized to view and use it [17].

The remaining sections of this work are organized as follows. The related work is covered in section II. In sections III and IV, we discuss the security and privacy concerns in Medical Internet of Things (MIoT) and the security and privacy requirement in Medical Internet of Things (MIoT). The cyber-attacks Faced by Medical Internet of Things (MIoT) are presented in section V. We present protocols security weaknesses in Medical Internet of Things (MIoT) in section VI. We are presenting the why favorite target for cyber attackers in healthcare sector in sections VII. We are discussing the possible countermeasures for security threats in Medical Internet of Things (MIoT) in sections VIII. We are widely discussing technical inadequacy in sections IX. In section X, we present challenges of security and privacy in MIoT. We conclude this paper in section XI. In section XII, we present the future of Medical Internet of Things (MIoT).

2. Related Work

Our healthcare systems today, all across the world, are based on a reactive sick-care model. The focus of the future generation will be on the individual and developing a proactive, preventative, and predictive treatment strategy. The Medical Internet of Things (MIoT) [20] is leading the way for healthcare applications to build a linked medical environment, improve systems [21], and enable patient's monitoring. This section discusses several techniques of using the Medical Internet of Things, as well as security and privacy concerns (MIoT). In the sphere of healthcare, there are several [22] sorts of uncertainty to consider while evaluating new programs [23] structural uncertainty, methodological uncertainty, variability, heterogeneity, and decision uncertainty are all examples of parameter uncertainty. This method is used to move some cloud computing tasks closer to smart devices in order to get faster processing while maintaining privacy [24]. Another technique is to describe the privacy support process of a trained SVM proposed. [25].

However, because it rejects Gaussian function responsibilities, this technique is limited to Gaussian kernels. Because the final SVM can induce information leakage regarding the final vector categorizing classes, this technique has a low accuracy rate. Qi et al. [26] looked at numerous IoT applications in smart healthcare from multiple angles (i.e., Blood pressure monitoring, monitoring of oxygen saturation, heartbeat monitoring etc.) [27]. Privacy, on the other hand, is more than a technical idea. In terms of both physical and information privacy, it is a fundamental human right. For selective access authorization and cryptographic secret sharing, the authors of [28] use Attribute Based Encryption (ABE). The EHRs are separated and reconstructed using a proxy. The different intrusion detection [29], authentication and authorization methods were given with little regard for their application to MIoT in order to ensure a secure IoT ecosystem.

Kernec et al. [30] proposed assisted living as a location of radar in the context of IoT for health, emphasising the importance of the setting. Yusuf Perwej and colleagues take a quick look at the technical components of IoT security. The security was a key problem when only two instruments were joined in the realm of medical treatment [31]. In countries across the Middle East and North Africa, cyber criminals exploit existing vulnerabilities in IoMT devices to obtain access to the medical care network and get unauthorized access to crucial healthcare data [32]. Lounis et al.[33] suggested a new cloud-based architecture for medical wireless sensor networks, as well as a security access control system that supports sophisticated and dynamic security rules and is based on cypher text policy attribute-based encryption (CP-ABE). A general survey on medical big data analysis was conducted in [34] to sort out big data issues and challenges of adopting MIoT solutions [35], while an on-demand IoT adoption in hospitals was conducted in [36] to improve nurses' experience based on the benefits and drawbacks of IoT adoption in healthcare technologies [37].

They studied the security-preserving SVM classification in [38], and while many earlier approaches had been offered, they were solely confined to safeguarding the training set

[39]. Informational privacy and confidentiality overlap in terms of allowed access or disclosure of information, as well as conceptions of secrecy, access-control, sharing, and information protection [40]. Turabieh et al. [41] used a dynamic L-RNN from artificial intelligence [42] to recover lost data from MIoT applications and provide good service quality for end users. Although computer security is an important pillar for establishing privacy, it is important to note that privacy cannot be achieved purely through security management [43]. To provide secure contact with the EHR system, [44] uses biometrics-based authentication and Kerberos ticketing sessions. EHR is also stored via a stenographic [45] approach. The main issues in the existing smart healthcare system were identified by Gong et al. [46]. Then they created a prototype system based on a lightweight private homomorphism algorithm and a DES-improved encryption technique. According to [47], using Blockchain as a security approach has various advantages, including allowing an agreement without the use of a trusted third party, avoiding the bottleneck, and ensuring that the antecedent medical data is complete and coherent. The security and privacy requirements for the MIoT are distinct from those for traditional networks, which are known as the CIA-triad (confidentiality, integrity, and availability) [48]. In [49], a Blockchain-based system for managing medical data was presented. It uses Ethereum smart contracts to handle data access permissions between entities such as patients [50], hospitals, doctors, research groups, and others [51].

3. Security and Privacy Concerns in Medical Internet of Things (MIoT)

The wider the network grows, the more beneficial it becomes in providing high-quality medical treatment, but it also makes its data more appealing to thieves. The ability to regulate when, how, and to what extent personal information is gathered, used, and disseminated is referred to as information privacy [52]. It has the potential to damage user confidence as well as people's lives. Connected systems in an IoT ecosystem can talk with one another, transmit data, and control it. In the dynamic world of IoT, the capabilities of system connections during various processes imply significant security and privacy challenges. One of the most groundbreaking breakthroughs in healthcare today is the Internet of Medical Things, commonly known as the MIoT. It allows doctors to keep an eye on patients from afar by giving them network-enabled devices. Every unprotected network-connected device in your environment is a security risk that, if left unaddressed, can lead to far more serious problems, such as patient health and safety [53]. IoT and MIoT devices, on the other hand, are notoriously difficult to secure, posing a serious security risk. Medical information is worth ten times more to hackers than a credit card number. The hospital is also vulnerable to a backdoor attack thanks to MIoT devices. Hackers infected blood gas analyzers, which are vital for the monitoring of critical care and surgical patients, in one well-publicized incidence. Attackers were able to access hospital networks and steal confidential data, which was subsequently sent to an unidentified destination, thanks to the infected devices. Even with proper precautions in place, the MIoT would be a risky position since it sends and receives incredibly personal data. Unfortunately, most modern systems are not designed to protect such sensitive information. In fact, due to the lack of security protections that most MIoT devices have by design, or due to inadequate security authentication methods that can be readily circumvented by a competent attacker, an attacker can eavesdrop and intercept incoming and outgoing data and information. Protecting the safety of medical devices and lowering the risk to healthcare networks, systems, data, and patients necessitates a multi-layered approach that goes beyond basic security hygiene. At all levels, including device, system, network, data, access, education, and governance, security threats must be analysed and handled. Because of the Internet of Things, there has been an increase in data security and liability threats in the healthcare industry. Many of the same security and privacy concerns apply to the Internet of Things, but it poses a far bigger risk because these devices operate [54] automatically. Healthcare organisations have also been subjected to more direct attacks in the past. Once a hacker has gained access to a network, they can use ransom ware to encrypt files or disable critical services until the firm pays a ransom. Because healthcare is such a time-sensitive industry, businesses frequently have no choice except to pay the ransom and hope that the funds are eventually recovered.

4. Security and Privacy Requirement in Medical Internet of Things (MIoT)

Although the majority of healthcare businesses do not devote enough resources to security and privacy, are unquestionably important in MIoT [55]. IoMT healthcare systems have more stringent security and privacy requirements than normal IoT-based infrastructures. MIoT devices generate a growing stream of increasingly diversified real-time data, all of which is extremely sensitive [56]. Each level of MIoT healthcare systems has distinct functionalities, which means each level has different security and privacy requirements. The following twelve requirements should be considered while creating medical Internet security and privacy systems.

4.1 Localization in MIoT

The process of calculating the positions of wireless devices in a network is known as localization. The former type of sensor localization is used to determine whether the sensors are in the correct bodily positions. For applications like activity recognition [57], such on-body sensor position identification is critical. Medical devices and MIoT healthcare systems may migrate in and out of network coverage on a regular basis. If the network's sensors depart and rejoin at irregular intervals, a real-time intrusion detection technique is necessary.

4.2 Data Integrity in MIoT

The quality and consistency (validity) of data throughout its lifecycle is referred to as data integrity. Attackers could use the wireless network's broadcast feature to get access to and manipulate patient data, which could have serious consequences in life-threatening situations. To ensure that the data has not been tampered with, the ability to detect any [58] unlawful data distortions or manipulations is essential. Domain integrity, referential integrity, entity integrity, and user-defined integrity are the four types of data integrity that can be maintained using foreign keys, constraints, rules, and triggers.

4.3 Access Control in MIoT

Access control is a way of controlling access to sensitive data, and effective access control schemes must be implemented to guarantee that only authorized devices and individuals have access to the medical servers. Because it is difficult to obtain a patient's permission or consent each time a data access request is made, medical server service

providers should provide selective access control for patients, allowing patients to choose which data can be shared without permission and which third parties can have access. Medical IoT servers should also be capable of quickly updating access control policies.

4.4 Data Usability in MIoT

Data usability is to ensure that data or data systems can be used by authorized users. Big data [59] brings not only great benefits but also crucial challenges, such as dirty data and nonstandard data.

4.5 Tamper Proof MIoT Devices

MIoT devices, particularly ambient sensors, can be physically taken, exposing security information to attackers [60]. At the very least, the MIoT medical devices in the systems should feature tamper resistant integrated circuits, which prohibit third parties from reading the codes placed on the devices once they have been installed.

4.6 Data Auditing in MIoT

A data audit is the process of examining data in order to determine its quality or utility for a certain purpose. Auditing MIoT data access is a good way to keep track of resource usage and a typical way to detect and track unusual events. Furthermore, cloud service providers frequently play untrustworthy roles, necessitating the use of realistic auditing procedures. Users, cloud service providers, access, and operation records are all examples of audit content.

4.7 Availability in MIoT

In the context of a computer system, availability refers to a user's ability to access information or resources in a specific location and format. If DoS attacks occur, services and data that are required by relevant users and delivered by medical servers and devices would become unreachable in the MIoT environment. Due to the risk of data loss, healthcare applications must be available at all times to assure data availability to users and emergency services.

4.8 Patient Privacy in MIoT

As opposed to secrecy, privacy is defined as a patient's right to be left alone and to make decisions about how personal information is disclosed. The information about patients can be separated into two categories: general records and sensitive data. Mental status, sexual orientation, sexual functioning, infectious diseases, fertility status, substance addiction, genetic information, and identification information are all examples of sensitive data [61]. We must ensure that sensitive information is not disclosed to unauthorized users or that even if data is intercepted, the information expressed is incomprehensible to unauthorized users.

4.9 MIoT Device Authentications

For data confidentiality and integrity, a device authentication mechanism should be able to establish secure and encrypted interactions [62]. Device authentication must be incorporated in any MIoT healthcare system because false information from malicious devices regarding patients' physical status could have serious negative consequences for clinical diagnosis and care decisions.

4.10 Data Confidentiality in MIoT

In health care, confidentiality refers to the obligation of professionals who have access to patient data or communications to keep that information private. An attacker can listen in on medical conversations and eavesdrop on data transmissions. Because the hacker can use the gathered medical data for a variety of illicit purposes, this eavesdropping procedure can pose serious risks to patients. Confidentiality [63] is defined as privileged communication between two parties in a professional relationship, such as a patient and a physician, nurse, or other clinical professional, as defined by law. We've learned to anticipate confidential communication from these connections as patients.

4.11 User Authentication in MIoT

Effective user authentication techniques are essential since the data kept on personal servers, whether temporarily or permanently, should only be accessed by patients and medical workers, such as caretakers [64]. Biometrics is a popular method for user authentication at the personal server level, and it's very useful in MIoT healthcare systems.

4.12 Data Freshness

An attacker can passively observe medical data as it is transmitted from patients to the appropriate doctor, and then replay it using old keys to confuse the coordinator. The term "data freshness" refers to the fact that the data is current and that no one can replay out-dated data. We distinguish between two forms of freshness. There are two types of freshness: weak freshness, which gives partial message ordering but no delay information, and strong freshness, which provides a total order on a request-response pair and allows for delay estimation. Sensor measurements necessitate weak freshness, whereas time synchronisation inside the network necessitates strong freshness.

5. Cyber Attacks Faced by Medical Internet of Things (MIoT)

The Medical Internet of Things (MIoT) and big data analysis constitute healthcare 4.0, which brings connection and data-driven decision making to routine healthcare procedures [65]. The Internet of Things is opening up a whole new universe of possibilities for improving the continuum of care. The Internet of Things (MIoT) extends beyond single-loop linear 1:1 network-connected medical devices. On the danger side, healthcare providers are becoming increasingly vulnerable to cyber threats as the number of linked and complicated medical devices grows. These attacks aim to compromise systems or component's confidentiality, integrity, availability, and authentication [66]. For many healthcare institutions, this is already an all-too-common reality. According to a recent survey, 83 percent of healthcare businesses have been victims of an IoT-related cyber assault in the previous year. During this span, ransomware targeting hospitals has been identified as the most common sort of attack. Healthcare organizations must defend their networks not only with PCs, laptops, and mobile devices, but also with medical device equipment [67]. To address this growing threat, healthcare institutions must maintain proper protection for their MIoT devices as well as excellent cyber hygiene.

5.1 Characteristics of Cyber Attacks in MIoT

It is critical to comprehend the characteristics displayed in figure 1 before detecting and classifying a specific attack. Internal & External Attackers, Malicious Attackers, [68] an active cyber-attack, a passive type attack, or a combination of the two, and Organized & Coordinated Attackers are all types of cyber-attacks that involve unauthorised access to private or confidential information stored on computer systems, medical devices, or networks. Attacks are classified according to how they attack. This classification aids in the identification of attack reasons and objectives, as well as proactive security planning in the MIoT. The state of digital security in the healthcare industry is currently critical. A data [69] breach results in much more than just a financial loss; it also causes your patients and staff to lose their sense of security.

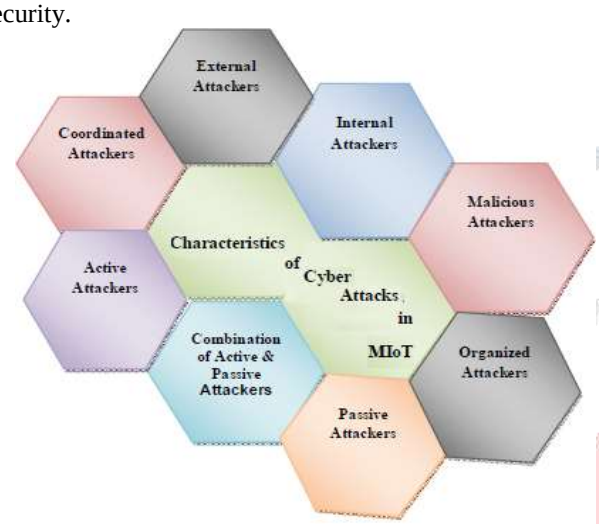

Fig. 1 The Characteristics of Cyber Attacks in MIoT

5.1.1 External Attackers

The bulk of external attacks involve malware such as worms, Trojan horse viruses, phishing, and other methods to steal personal information. A backdoor or key logger will be installed on the machine once it has been downloaded. The main goal is to compromise patients' privacy and sell their information to malevolent third parties for scamming purposes on the deep dark web.

5.1.2 Internal Attackers

When an individual or a group within an organization attempts to disrupt operations or exploit organizational assets, this is known as an internal attack. In many circumstances, the attacker uses a large amount of resources, tools, and experience to conduct a sophisticated computer attack, as well as potentially removing any proof of the attack. It might be a spy posing as a nurse or a doctor who was able to effectively bypass all of a hospital's security systems in order to eliminate a patient for political or other illegal reasons.

5.1.3 Malicious Attackers

Malware attacks occur when cybercriminals produce malicious software that is installed on another person's device without their knowledge in order to obtain personal information or damage the device, usually for financial benefit. They initiate assaults merely because they can, with the goal of causing havoc with a MIoT system.

5.1.4 Active Attackers

Active cyber-attacks are often clear, forceful attempts that victims become aware of right away. Active assaults are usually very malevolent, locking users out, deleting memory or files, or forcing access to a targeted system or network. When used to inject a patient with a greater dosage of a medicine, or when prescribing the incorrect drugs, such an attack is extremely dangerous, putting patients' [70] lives in jeopardy. Hackers that use active assaults are usually unconcerned about their operations being noticed because the damage has already been done or is in progress by the time the attack is discovered.

5.1.5 Passive Attackers

Non-disruptive and covert approaches are frequently used in passive cyber-attacks so that the hacker does not draw notice to the attack. The goal of a passive attack is to get access to medical equipment, computers, and networks in order to gather data without being detected. The goal is to intercept data sent between different medical equipment via any wireless communication, read it, and develops their own information gathering mechanism that may be utilized for further exploitation, potentially leading to a far more sophisticated cyber-attack. The information obtained in a passive cyber-attack is frequently sold on the black market or the dark web for the benefit of the person who carried out the attack.

5.1.6 Organized Attackers

Before starting a cyber-attack on a medical equipment or system, planned attacks are usually based on having prior knowledge of it. In reality, the goal is to get unauthorised access or to reveal sensitive information.

5.1.7 Combination of Active & Passive Attackers

To acquire unauthorised access to a system, medical equipment, or data, many hackers employ a combination of active and passive tactics. Often, a hacker may utilise a passive data collection technique first, and then, once the needed data has been acquired, the hacker will launch an active attack to prove a point or achieve some other aim. For example, it is fairly uncommon for a hacker to use a passive attack strategy to get login credentials before aggressively accessing the system and wreaking havoc on the network.

5.1.8 Coordinated Attackers

The coordinated attacks are predicated on insiders and outsiders cooperating and collaborating. Insiders are rogue and disgruntled employees (Hospital IT, staff, nurses, receptionists, and so on) who have authorised access to the system and may install malware. The attack might be carried out to disrupt medical operations by preventing authorised medical workers and patients from accessing medical records, booking appointments, and disrupting medical procedures.

5.2 Cyber Attacks in MIoT

Hackers stealing sensitive health information and a rising epidemic of COVID-19 infections [71] are two examples of things we can't control in today's society. In the past, sophisticated, state-sponsored attacks were frequently directed at healthcare. Amateur hackers carrying out basic,

generic assaults on non-medical gadgets that happen to be connected to clinical networks might now inflict substantial harm due to the healthcare industry's susceptibility. Every day, hospitals must be prepared for a range of spontaneous attacks. With various IoT devices connected to the hospital's network [72] that lack security, they will undoubtedly serve as the preferred entry point for hackers looking for a quick way in. The COVID-19 epidemic has wreaked havoc on healthcare organizations, such as hospitals and medical research facilities, and cyber thieves have taken advantage of the situation [73]. In this section, we'll look at some of the cyber assaults that have been launched against the MIoT.

5.2.1 Eavesdropping

Eavesdropping attacks are primarily based on information collection and are classified into two types first passive eavesdropping and second active eavesdropping. Assailants are finding this to be one of the simplest ways to obtain data from the sensors indicated in figure 2. Attackers track down the necessary hardware and intercept it, allowing them to successfully collect data from hardware devices. During transmission, for example, a patient's vitals [74] may be intercepted. Data gathered in this manner unlawfully can be used to carry out a variety of attacks. Even though encryption can solve this problem, it is not always feasible, especially with low-powered devices.

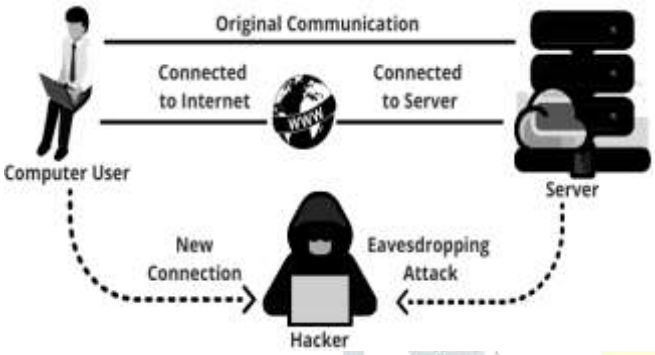

Fig. 2 The Eavesdropping Attacks in MIoT

5.2.2 Replay Attacks

A replay attack is a type of man-in-the-middle assault in which an attacker sniffs communications being delivered over a channel in order to intercept and resent them as genuine messages. An attacker could re-use an authentication message that was previously sent between two legitimate users. Eavesdropping or hacking some of the nodes could have allowed the attacker to intercept the communication. Because it lacks secure communication methods, the insulin pump OneTouch Ping, for example, is known to be vulnerable to this attack. Physical harm to a system, particularly medical systems, can be achieved in several instances. System communications are first captured, then replayed' to the receiving device later [75]. This can lead to unlawful access and enhanced privileges on a medical system by stealing, leaking, or revealing critical information.

5.2.3 Reverse Engineering Attacks

An attacker will often download the targeted software from an app store and evaluate it using a variety of tools in their own local environment. A person-to-person attack is another name for a reverse social engineering attack [76]. This allows the attacker to pose as a technician attempting to resolve a problem with a hospital's medical system in order to obtain access to the system and get information. It also enables him to potentially upload malware or find exploitable holes.

5.2.4 Rogue Access Attacks

In this attack, a forged gateway is set up within the wireless network range to allow legitimate user access and in turn, intercept traffic. According to the SANS Institute, this attack can be executed using free software and cannot be easily discovered because a forged gateway may hide its presence.

5.2.5 Masquerading Attacks

A masquerade attack is an attempt to get unwanted access to personal computer information by impersonating someone else's identity, such as a network identity. A masquerade attack can make an authorization process exceedingly vulnerable if it is not adequately secured [77]. For example, by impersonating the legitimate user, the attacker might take the user's terminal device (e.g., smartphone) login credentials and obtain unauthorized access to stored confidential health data. Through the insertion of rogue devices, an attacker might impersonate a legitimate user to get access to services provided by the MIoT device, or an attacker could appear as a MIoT device to offer fraudulent services to consumers. In the second scenario particularly risky in the healthcare industry, where MIoT devices deliver life-saving services to patients.

5.2.6 ZED Sabotage Attacks

The developers of this attack suggest a novel ZigBee protocol attack called as a ZigBee End- Device. The main goal of such attack is to vandalism the [78] ZED by sending periodically a particular signal to wake up the object to drain its battery.

5.2.7 Dumpster Diving Attacks

The process of exploring trash for useful information about a person and medical information that can later be used for the hacking purpose indicated in figure 3 is known as dumpster diving. This assault primarily targets large healthcare organisations or businesses, with the goal of phishing (mainly) by sending victims phoney emails that look to come from a legitimate source. During this attack, any medical information, including patient records, medical prescriptions, staff names, and other papers and files tossed in the garbage, is retrieved.

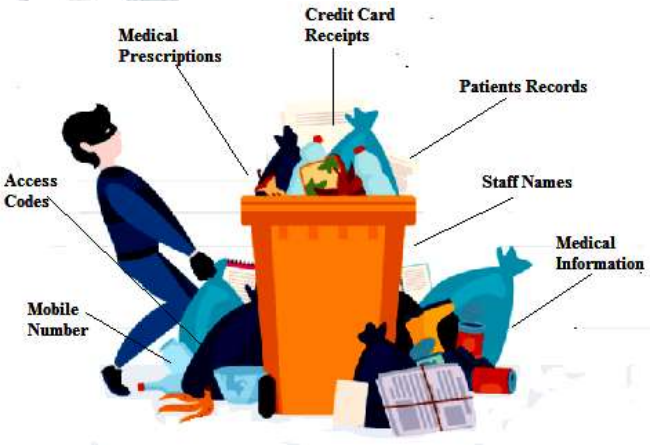

Fig. 3 The Dumpster Diving Attacks in MIoT

5.2.8 Traffic Analysis Attacks

This attack primarily affects patients' privacy as well as the confidentiality of their data. This is a very risky attack that involves intercepting and analysing network traffic patterns in order to derive relevant information. This is because the actions of MIoT devices can possibly provide enough

information to allow an adversary to harm medical devices maliciously.

5.2.9 Message Tampering Alteration Attacks

The Message Tampering Alteration attack is based on modifying application data such as user credentials and permissions, pricing and number of products, and so on by manipulating parameters transmitted between client and server. The attacker's goal is to compromise the data integrity of the communications being exchanged. This occurs when an attacker manipulates received messages to achieve his or her own objectives [79]. As a result, doctors will make poor decisions that could jeopardise patients' health.

5.2.10 Malicious Data Injection Attacks

This type of assault is launched by an entity that is either lawful or has the ability to authenticate with the system. As a result, by sending a false message to the hospital data centre or clinicians, this can have dangerous consequences in the MIoT system, potentially leading to tragic accidents [80]. The goal of this attack is to prevent authorised users from sending actual and correct messages, instead injecting fraudulent messages into the network.

5.2.11 Data Availability Attacks

By dropping these messages, the attacker hopes to disrupt the data availability of the exchanged messages. This occurs when an attacker manipulates received signals for his or her own purposes, causing the hospital data centre or doctors to miss critical information about the patients' health state.

5.2.12 Denial of Service (DoS) Attacks

DoS attacks are undertaken in order to disrupt the availability of a specific medical IoMT system or device, preventing legitimate patients from receiving necessary prescriptions and nurses and doctors from obtaining medical information and data. The disturbance and interruption of service prohibits real-time data from being transferred and received. Dos attacks take use of flaws in application interface programmes (API).

5.2.13 Sinkhole Attacks

In WSNs, this type of attack is more common. A rogue node draws traffic by offering improved link quality in this attack (e.g., advertising fake routes). Once traffic has been drawn to the rogue node, further attacks such as eavesdropping or selective forwarding, in which the malicious node isolates particular nodes by deleting packets passing through them, can be launched.

5.2.14 Distributed Denial of Service (DDoS) Attacks

These attacks can even be carried out at the same time from different geographical regions and countries. This can have a significant impact on the availability of medical devices and systems, resulting in a detrimental impact on the lives of patients due to the inability to respond quickly. The flooding of a resource with so many requests, for example, is an example of this assault.

5.2.15 Fragmentation Attack

Fragmentation assaults are a frequent type of denial of service attack in which the attacker uses datagram fragmentation methods to overwhelm a network. Unlike IPv6, which has a minimum MTU of 1280 bytes, IEEE 802.15.4 objects have a maximum transmission unit (MTU) of 127 bytes [81]. 6loWPAN allows IPv6 packets to be sent over IEEE 802.15.4 thanks to its fragmentation method. An attacker can put his fragment into the fragmentation chain because it is constructed without any sort of authentication.

5.2.16 Wireless Jamming Attacks

The attacker intends to significantly disrupt any existing wireless medical device connectivity between patients and hospitals. Wireless networks, in particular, have been heavily targeted [82] by a series of continuous denial of service assaults, which disrupt every communication attempt on secure and non-secure channels, depending on whether the jamming attack is selective or non-selective.

5.2.17 Cross-Site Request Forgery Attacks

This type of attack is more widespread in IoT systems that use RESTful APIs. The CSRF technique deceives the end user into acting on a susceptible application without their knowledge. The web interface of the IoT layer becomes vulnerable to the CSRF attacks if not configured properly.

5.2.18 ICMP Flooding Attacks

An Internet Control Message Protocol (ICMP) flood or Ping flood attack with a Denial-of-Service (DoS) capability overwhelms a targeted medical device with ICMP echo-requests known as pings is used in these attacks. To carry out such assaults, attackers use exploited MIoT devices (zombies or bots) that are managed by a bot master.

5.2.19 TCP Hijacking Attacks

This type of attack is used to keep track of a TCP connection. In this instance, an attacker can discover and guess the conveyed entities' sequence numbers and checksums [83]. The attacker can then inject a malicious TCP packet with the check-sum and sequence numbers that the receiver expects, as the receiver lacks a way to validate the packet source and deem it legitimate.

5.2.20 Half Open Attacks

Because high-capacity IoMT devices rely on Transmission Control Protocol (TCP) services to communicate (i.e. email and web servers), this attack primarily targets them [84]. The goal of this attack is to crash a medical server by depleting the memory reserve of the e-Healthcare server, allowing insecure connections to be used for future attacks.

5.2.21 SQL injection Attacks

An SQL injection attack occurs when an attacker attempts to target the application's backend database by entering a faulty SQL statement. This assault offers a serious threat to IoT devices, particularly in the healthcare industry, because a successful SQL injection attack can compromise sensitive patient data or alter important data. SQL injection vulnerability in a cardiac management system has been discovered.

5.2.22 Pre Shared Key Attacks

The security mechanism in some IoT applications, such as the CoAP protocol, is based on pre-shared keys in this attack. These keys are sometimes hard coded into the programming. As a result, if the attacker gets access to the library files, he can quickly gain access to them [85].

5.2.23 Black Nurse Attacks

The black nurse attack is a series of low-bandwidth (15-18 Mbit/sec) ICMP denial-of-service assaults that target firewalls with high Central Processing Unit (CPU) loads [86]. This attack results into preventing Local Area Network (LAN) users, including patients and medical staff from transmitting internet network traffic.

5.2.24 Account Hijacking Attacks

Many IoT devices used in this assault communicate in transparent text over the network or have inadequate encryption. By intercepting the packet when an end user is being authenticated, an attacker can accomplish account hijacking. The key factor in the growth of this attack, as documented in many occurrences, is old operating systems with unpatched vulnerabilities.

5.2.25 Man-in-the-Middle Attacks

One of the most common authentication attacks, this one controls and monitors communication between two legitimate parties while modifying the data sent. This might be a passive or active attack. When the attacker just intercepts and reads the exchanged messages between the two entities, it is considered a passive attack. On the other hand, if the attacker is able to alter, manipulate, or/and modify the sent data or information without the awareness of the devices, it is considered an active attack.

5.2.26 Sensor Tracking Attacks

In the event of an emergency, sensors in patient monitoring equipment with GPS sensors, fall detection, or wheelchair management will broadcast the patient's location to the doctor or monitoring institution. Attackers can gain access to the patients' whereabouts, sensitive data, or even send incorrect data by hacking into these devices [87].

5.2.27 Blue Bugging Attacks

Bluetooth devices [88] are vulnerable to a variety of attacks in this attack, the most dangerous of which being bluedugging. By exploiting vulnerability in old device firmware, an adversary might gain access to the victim's device and spy on phone calls, send and receive messages, and connect to the internet without the lawful user's knowledge [89].

5.2.28 Dictionary Attacks

When attempting to obtain access to a medical system, this type of attack is most common. When security measures are less stringent than the security measures of a given IoT device, attacks are more likely to succeed. Such attacks rely on a huge set of dictionary words to guess the password and obtain access to the system [90]. In truth, such an attack is resource and time intensive, taking anywhere from minutes to hours, and even days to complete.

5.2.29 Rainbow Table Attacks

This attack uses reverse engineering to primarily target the password and its hash value, based on a technique known as "fault and trial." It typically contains a table of passwords and hashes that is performed until a match is found. Different solutions to this problem were provided in [91]. Salt passwords, on the other hand, can be an excellent way to protect against these types of assaults.

5.2.30 Session Hijacking Attacks

This attack is carried out with the help of a session sniffer, which is a packet sniffer capable of modifying, recording, and reading network traffic (header and data) between two parties. This applies to both individuals and gadgets. This exploit can, in fact, capture a legitimate session ID (SID).

5.2.31 Birthday Attacks

Users that rely on weak hashing systems, where two different passwords can have the same hash, are likewise vulnerable to birthday assaults. Such flaws are easily exploited in order to get unauthorised access to any medical system. In, there was a suggested hash function balancing. Secure Hash Algorithm (SHA-3 and SHA-512) techniques, on the other hand, remain the best defence against such assaults.

5.2.32 Elevation of Privilege Attacks

Elevation of privilege refers to an attacker's ability to get crucial, limited access to a system and then enhance their privileges, or what a user is allowed to do subsequently [92]. By promoting themselves to higher level accounts that can make more changes to the system, they will be able to gain access to information and systems that they would not otherwise have access to. An attacker with privileged read-only capabilities, for example, can raise the set to include read and write permissions. Therefore, an elevation of privilege attack is when a user receives privileges they are no ten titled to.

5.2.33 Spyware Attacks

A spyware's main objective is to collect and acquire information about patients in order to give it to a third party or sell it on the dark web. This is accomplished by placing users under constant supervision [93]. In fact, spyware may gather enough information about a patient to allow for assassination. They can also be used as key loggers to steal the credentials of patients.

5.2.34 Ransomware Attacks

IoT ransomware receives insufficient attention, which might have disastrous consequences as compared to regular malware. The most IoT data is stored in the fog or cloud rather than at the device level, the traditional ransomware paradigm is just not possible. IoT ransomware encrypts IoT devices [94] and demands a ransom from their owners in order to unlock them. Unfortunately, ransomware is a popular target for MIoT devices [95]. We are locking the operations of some devices, such as pacemakers and drug infusion pumps, can have disastrous consequences since patients might be gravely injured or even die if these devices are not unlocked in a timely manner.

5.2.35 Information Disclosure Attacks

Unauthorized access to private data such as patient information compromises the MIoT system's security. An attacker could use some of the previously listed methods, such as CSRF and session hijacking, to get unauthorised access to sensitive information. In 2018, about 52% of healthcare breaches were of this type.

5.2.36 Worm Attacks

In the case of the MIoT, worms are most likely the most damaging and hazardous sort of malware. Worms are a type of malware that uses existing weaknesses in a connected device to self-replicate vertically Mover [96]. As a result, they can self-propagate without the need for human involvement. They can affect the security services (confidentiality, integrity, and availability) of all data and devices, potentially resulting in crucial data loss or life threats.

5.2.37 Configuration Attacks

Attacks are frequently carried out by taking advantage of any misconfiguration or implementation fault that went unreported during the setup of the MIoT system. For example, if a firewall is not installed in the link between MIoT devices and the cloud, the attacker can intercept the data.

5.2.38 Botnet Attacks

These attacks rely on exploiting flaws in MIoT devices to transform them into bots that wait for commands from the adversary via command-and-control to provide bogus or incorrect information about patients. They can also be employed in DoS or DDoS assaults to bring the entire medical system down [97]. In fact, many of these assaults are focused at exposing sensitive data and exploiting it for malicious or personal benefit.

5.2.39 Side Channel Attacks

Most IoT objects will be integrated with security methods such as encryption to secure their sensitive data for security reasons. The side channel attack, on the other hand, analyses side channel information emitted by IoT items in order to break such mechanisms. Some examples of such attacks are power and time analysis attacks [98].

5.2.40 Remote Access Trojan Attacks

In this attack, a medical system's vulnerability, weakness, or security gap in a targeted medical system is exploited. Such attacks rely on acquiring covert illegal access as a backdoor to get around all security procedures and countermeasures. As a result, all of the security measures in place are defeated. Timing Attacks are side channel attacks in which an attacker analyses the required execution time of cryptographic algorithms in order to compromise a cryptosystem. Furthermore, a timing attack is a type of security exploitation in which an attacker discovers security flaws in the computer or network system.

5.2.41 Brute Force Attacks

A brute force attack involves guessing login information, encryption keys, or locating a hidden web page by trial and error. Hackers try all conceivable combinations in the hopes of making the right guess. The cyber equivalent of trying every key on your key ring and eventually finding the appropriate one is a brute force attack (also known as brute force cracking). Brute force attacks were responsible for 9% of confirmed data breaches in 2019. This basically entails trying all feasible possibilities to guess inputs such as passwords. Because there is insufficient protection in place to stop such assaults in IoT devices, MIoT apps are vulnerable to brute-force attacks. The sensors' simulated compute power is to blame for this.

5.2.42 Firmware Based Attacks

Firmware hacks, while not as well-known as ransomware, worms, and Trojans, are especially harmful and capable of circumventing regular antivirus software by infecting your device's lower stack [99]. Companies like Microsoft, Samsung, and Google, for example, have built in the ability to update their vulnerabilities remotely when they are discovered. MIoT systems, on the other hand, are rarely designed to receive regular upgrades because they are built by offshore third parties. The majority of these third parties do not have skilled developers on staff to safeguard these systems. Worse, the bulk of MIoT devices have no way of being updated.

5.2.43 Medjacking Attacks

Hacker gains access to a system via a backdoor constructed by hijacking a medical device in the Medjacking attack vector. Because of the rising targeting of healthcare systems, a new term for these cyber-attacks has been coined medjacking in figure 4. However, medjacking can be used for more than just gaining access to a patient's medical records. Vulnerabilities in medical devices may endanger patients' health, if not their lives. The attackers can utilize the backdoor to steal patient data, send ransomware, or shut down systems once it has been setup. The goal of every Medjacking attack is to get access to the hospital's network.

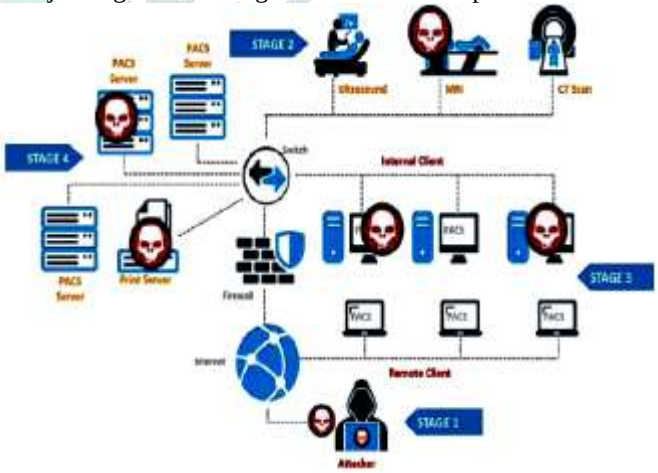

Fig. 4 The Medjacking Attacks in MIoT

5.2.44 Cryptojacking Attacks

Cryptojacking is a new sort of cyber security threat that uses a compromised device's processing capacity to mine Bitcoin on behalf of the hacker. Cryptojacking can have a severe influence on a hacked device's operation and shorten its lifespan. Cryptojacking could jeopardise patient safety in a hospital setting where various medical equipment are employed for patient care.

5.2.45 *Advanced Persistent Attacks*

For many businesses, advanced persistent threats constitute a big security risk. A targeted cyber-attack in which an intruder gains unauthorized access to a network and remains undiscovered for an extended length of time is known as an advanced persistent threat. Using advanced persistent threats, attackers hope to monitor network activities and steal vital data. It is difficult to prevent, detect, or neutralize such cyber-attacks. These MIoT devices can be used by cybercriminals to obtain access to personal or corporate networks. Cybercriminals can steal confidential information using this method.

5.2.46 De-Synchronization Attacks

TSCH stands for Time Synchronized Channel Hopping and is defined in the IEEE 802.15.4e standard. Low-power gadgets employ TSCH to communicate over a wireless network. It is intended for use in low-power, lossy networks (LLNs), and it attempts to provide a dependable Media access control layer. Through time synchronisation and channel hopping techniques, it achieves great consistency and has low duty cycles. Attacks on the TSCH time synchronisation can occur when an attacker sends messages during the time slots reserved for other users. As a result, the packets clash and are lost. An attacker can trigger a succession of these events by carefully analysing the back-off times, eventually causing the nearby motes to become de-synchronized. As a result, this assault can be described as a more complex variant of the collusion attack.

6. Protocols Security Weaknesses in Medical Internet of Things (MIoT)

Varied technologies with different features for different applications may power the Internet of Things (IoT). Security is a secondary feature of IoT protocols, which are primarily designed to be energy efficient and to efficiently handle node connectivity in complicated ad-hoc contexts. The Medical Internet of Things (MIoT) is one of the most practical and valuable applications of the Internet of Things (IoT), allowing medical devices and apps to be connected to an online healthcare system [100]. MIoT applications frequently rely on a variety of technologies with varying embedded features, each with its own set of security concerns. The protocols security flaws in the Medical Internet of Things (MIoT) are discussed in this part, as illustrated in table 1.

6.1 Z-Wave

The Z-wave is a new type of wireless technology that allows smart devices to connect with one another. A standard key exchange procedure is not enforced by the Z-Wave protocol. Attackers have been found to take advantage of custom key setup processes [101]. Researchers discovered a Z-Wave implementation that may be hacked by abusing the unique key setup protocol and a feature that allowed numerous protocol executions for a single device in 2013. Impersonation and node spoofing attacks to escape network checks, as well as Black Hole attacks, are further attacks on Z-Wave equipped devices. By spoofing frames coming from the controller or another device, impersonation attacks can impersonate device sources.

6.2 HL7

HL7 was created in an unsecure manner. HL7 security problems are related to implementation concerns because no severe security measures are implemented. Various encryption and authentication flaws have been discovered in ad hoc security mechanisms applied in various implementations. Lack of authentication allows rogue devices to impair network functionality by sending faulty ACK messages, which is another type of attack on HL7 networks.

6.3 Wi-Fi

Wi-Fi is a wireless networking technology that connects devices to the Internet, including computers (laptops and desktops), mobile devices (smart phones and wearable's), and other equipment (printers and video cameras). The lack of granular device authentication, the minimal protection of service integrity besides encryption, and the protocol's fundamental weakness against denial of service attacks on the wireless network and signal itself are the most common security flaws of the Wi-Fi protocol. These can be aimed at different layers of a Wi-Fi implementation for denial-of-service attacks. Peer-to-peer and eavesdropping attacks are also common on medical Wi-Fi networks, because linked equipment are exposed to other devices on the same network.

6.4 6LowPAN

Wireless sensor networks are one of the many uses for the 6LoWPAN system. This type of wireless sensor network uses IPv6 and sends data in packets, hence the term IPv6 over Low Power Wireless Personal Area Networks. Sensors and Medical Internet of Things (MIoT) devices can use 6LoWPAN wireless modules for secure low-power connectivity. 6LowPAN attacks are directed at either the IP network or the radio signal. The employment of malicious intermediary network nodes to attack a 6LowPAN network from the inside is one type of attack. Signal jamming, replay attacks to create address depletion, and flooding attacks to cause DoS against legitimate devices are examples of such attacks. 6LowPAN has flaws in its fragmentation process as well. In [102], the authors discovered two design-level flaws that allow attackers to deliberately impede accurate packet reassembly on target nodes using a single protocol fragment.

6.5 AMQP

AMQP (Advanced Message Queuing Protocol) is an open standard for exchanging business communications between applications or organizations. It connects systems, provides information to corporate processes, and reliably communicates instructions to help them achieve their objectives. The protocol has advanced features and is now utilized in a variety of circumstances where dependable asynchronous communication between endpoints is required. Access control, message and identity validation, and message queue management are all affected by these vulnerabilities, which mostly affect the broker component. Privilege escalation, information exposure, Denial of Service attacks, authentication and authorization bypass, remote code execution, and traffic hijacking are all possible outcomes of these vulnerabilities. Other security issues that concern AMQP setups have to do with broker settings. In fact, despite the presence of a web user interface, AMQP brokers are extremely sophisticated, and setting them up can be difficult.

Mistakes in the configuration of message queues, exchanges, producers, and consumers might result in major vulnerabilities [103].

6.6 RFID

The use of radio waves to read and collect information recorded on a tag connected to an object is known as radio-frequency identification (RFID). Confidentiality attacks on the physical and network layers are possible in RFID. The majority of attacks raise concerns about data confidentiality and location privacy. Attackers can frequently breach sensitive health data recorded in tag data related to treatments. Because of their passive nature, even solutions like encrypted RFID implementations are known to be vulnerable to side channel attacks [104].

6.7 CoAP

The Constrained Application Protocol (CoAP) is a customized web transfer protocol designed for usage in the Internet of Things with constrained nodes and networks (IoT). The Datagram Transport Layer Security (DTLS), which is the official security protocol for CoAP, is used in combination with the CoAP. DTLS has its own set of security issues, such as big messages and handshake compression, and is incompatible with CoAP proxy modes [105]. An attacker can leverage end devices to turn a tiny packet into a bigger packet and perform DoS attacks using amplification attacks. Amplification attacks can be mitigated by employing blocking and slicing modes on CoAP servers.

6.8 UWB

Ultra-wideband (also known as UWB, ultra-wide band, or ultra-band) is a wireless communication technology for short-range communication. It employs radio waves to allow devices to communicate with one another. Does this ring a bell? Yes, it's similar to Bluetooth, but it's more accurate, dependable, and efficient. UWB impulse radio, which is specified as 802.15.4a,f, has become a popular method for precise range. UWB is vulnerable to physical layer attacks, such as the early detection and late commitments (ED/LC) attack described by Singh et al. [106], because it is a distance-based protocol.

6.9 IrDA

Infrared data association (IrDA) is a collection of device makers who produced a standard for data transmission using infrared (IR) light waves. It contains specifications for the entire family of wireless IR communication protocols. IrDA allows for point-to-point communications and requires direct line-of-sight communication between two infrared sensor equipped devices. Even for the most basic security measures, infrared technology lacks technological backing. By intercepting reflected infrared light and filtering out the surrounding ambient noise, attackers can eavesdrop on data delivered despite its short range [107].

6.10 ZigBee

The ZigBee wireless technology is essentially a publicly available global standard for low-power, low-cost wireless M2M (machine-to-machine) networks and the Internet of Things (IoT). It uses the IEEE 802.15.4 physical radio standard and may operate in unlicensed bands such as 2.4 GHz, 900 MHz, and 868 MHz. For all devices on a particular network and all layers of a device, ZigBee permits key reuse between layers of the same device and utilizes the same security level [108]. The exploitation of ZigBee can be divided into two categories: implementation and protocol flaws. The majority of ZigBee's protocol vulnerabilities are inherited from 802.15.4. There are no integrity checks in acknowledgement packets (ACKs), merely sequence numbers that can be easily intercepted. Another ZigBee vulnerability discovered takes advantage of the lack of verification in device PAN IDs. This allows attackers to reset all device network connections to factory defaults.

6.11 XMPP

Extensible Markup Language Protocol (XMPP) is a messaging protocol based on it (XML). RFC 6120, RFC 6121, and RFC 7622 of the Internet Engineering Task Force (IETF) have standardized the eXtensible Messaging and Presence Protocol (XMPP). Asynchronous Messaging, Publish & Subscribe, and Request & Response are among the communication patterns supported by the protocol. Extensible Messaging and Presence Protocol (XMPP) is an open XML technology that allows two or more entities to communicate in real time. Despite this, the protocol's lack of end-to-end encryption renders it open to a variety of threats. An attacker might, for example, edit, delete, or replay stanzas or gain unauthorized access to a server. Aside from the protocol's security flaws, a slew of vulnerabilities plague XMPP-based applications and services. Custom functionalities that can be readily implemented on top of the XMPP protocol are linked to other vulnerabilities. Implementations of an extension used for sending user avatar information allow attackers to compromise data location, as stated in [109].

6.12 NFC

NFC is a standards-based wireless communication technology that enables safe two-way interactions between electronic devices across short distances. Communication is created in a straightforward manner, with no user setup required, as is the case with many other wireless connections. As a result, simply tapping two devices together, consumers can conduct contactless transactions, access digital content, and connect electronic gadgets. NFC (Near Field Communication) is a radio frequency regulation system that allows data to be sent between two devices in close proximity. The NFC standard does not provide any safeguards against proximity attacks. Typical Man-in-the-Middle (MITM) assaults use simple antennas can result in data breaches or signal corruption, resulting in integrity or Denial-of-Service attacks. In certain types of NFC card modulation, NFC is also vulnerable to DoS and data alteration attacks, either through signal corruption or bit manipulation [110].

6.13 WIA-PA

WIA-PA employs a topology that combines peer-to-peer and star [28]. Each routing device can lead its own star, and the routing devices communicate with each other in a peer-to-peer topology. Only the 2.4 GHz frequency range and a data rate of 250 kbps are supported by WIA-PA. WIA-PA is a security standard that protects against attacks like eavesdropping and traffic analysis. On WIA-PA, Dos attacks can be used during non-encrypted join requests [111]. The attacker can keep delivering faulty packets by recalculating the cyclic redundancy check (CRC). The receiver is

overworked as a result of having to execute integrity checks every time a packet is sent.

6.14 Bluetooth

Bluetooth is a short-range wireless technology standard for transmitting data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, ranging from 2.402 GHz to 2.48 GHz, as well as for establishing personal area networks (PANs) [88]. The payload of a Bluetooth transmission is encrypted, not the entire packet. For identical functions, such as device model verification and service listing, many medical devices use the same interface type and specific channels. Another method involves matching the frequency hops of a Bluetooth connection and then capturing data in that frequency range. For MITM confidentiality attacks, such attacks can sniff and collect Bluetooth transmissions [112]. Despite the fact that existing implementations of the protocol provide some security safeguards against MITM (as previously indicated), researchers have discovered flaws.

6.15 MQTT

MQTT (Message Queuing Telemetry Transport) is an IBM-developed lightweight messaging protocol that was initially introduced in 1999. It interprets communications between devices, servers, and applications using the pub/sub pattern. MQTT includes numerous data encryption and authentication techniques [113], However they are not given or configured by default. The security of the MQTT protocol is based on an authentication method that lacks encryption capabilities [114]. Traffic analysis can be used by attackers to obtain important information from data in transit. Personal Data Protection MQTT does not include an inbuilt data encryption mechanism by default. Whether the broker device (the master device that handles traffic in the MQTT protocol) utilizes authentication or not, the data exchanged between the broker and a simple IoT device node can still be sniffed by an attacker.

6.16 mDNS

The multicast DNS (mDNS) protocol is a name resolution protocol for smaller networks. It does it in a way that differs from the well-known DNS. Instead of asking a name server, all network participants are addressed directly. The suitable client broadcasts a multicast message to the network, inquiring which network member matches the host name. The Multicast Domain Name System (mDNS) is an open protocol for service discovery and name resolution on local networks. This protocol, when combined with DNS-based Service Discovery (DNS-SD) [115], provides the flexibility needed in contexts where new devices must be immediately integrated and DNS-like activities must be performed without the use of a traditional DNS server. Attackers spoof mDNS answer messages and promote false services in this protocol, which is routinely abused for additional assaults against uninformed nodes. Again, attackers take advantage of mDNS equipped nodes responding to external queries to misuse services for a variety of objectives, including Distributed Denial of Service reflection assaults and data harvesting.

6.17 ISA 100.11a

The ISA100.11a standard was intended to offer non-critical monitoring, alerting, and control applications with dependable and secure wireless operation. ISA100.11a is a standard that defines security features for IEEE 802.15.4 wireless networks. It's designed for low-data-rate wireless communication with fixed, portable, and mobile devices that have very low power requirements. 6LoWPAN, IPv6, and UDP are used in its network and transport levels [116]. As a result, end-to-end encryption is provided by the ISA 100.11a transport layer. The aforementioned technologies have inherent vulnerabilities, which could lead to security risks. Another key thing to remember is that the ISA protocol typically connects devices with unique properties that attackers can exploit [117]. Devices, for example, have limited storage capacity, computing power, bandwidth, and connection capabilities, all of which can be used by attackers to launch DoS attacks.

6.18 HTTP

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for hypermedia information systems that are dispersed and collaborative. HTTP is an application layer protocol that runs on top of other layers of the network protocol stack to convey data between networked devices. HTTP is insecure by default, making it vulnerable to common attacks such as eavesdropping, injection, and manipulation. HTTP implementations by default are not encrypted. End-to-end encryption is achieved using HTTPS (encrypted HTTP). Low and slow rate attack: In this assault, an attacker sends fraudulent HTTP traffic at a very low rate to prevent detection by intrusion detection systems [118]. In the Internet of Things, such attacks frequently attempt to deplete the energy of devices.

Table 1. The MIoT protocols security features, data rate, topology, vulnerabilities, spectrum, attacks

Protocol	Security Features	Data Rate	Topology	Vulnerabilities	Spectrum	Attacks
RFID	Embedded data are unprotected and read only	106–424 Kbps	Star, Ring	Active (continuously transmitting) and passive RFID systems suffer from weaknesses	13.56 MHz	Side channel attack
Bluetooth	Secure simple pairing (SSP), Connectivity issues over obstacles	1, 2, 3 Mbps	Star, Point – to -point	Encryption of the payload and not of all the entire packet, matching the connection's frequency hops, then capturing data in that frequency range	2.4 GHz	Sniffinig, DoS, MITM, Brute-Force, device duplication attacks
ISA100.11a	Linchpin, AES-128, time limitations	250 Kbps	Mesh topology	Requires some special conditions to be implemented in a secure path	2.4GHz	Sniffing, Spoofing, Replay attacks and data falsification
AMQP	Encryption and authentication by x.509 certificates, Make a scan to	45 Mbps		End-user-developed modules can be insufficient regarding threat-mitigation and can make the end product vulnerable to		An attack entity replays data between communication session to impersonate

	discover open brokers			cyber-attack		a user to obtain information, deletions to the network communication content
LoRaWAN	128-bit application session key (AppSKey), AES	300 Bps - 37.5 kbps	End – to -End	Resetting frame counters without re-keying, caching and replay of ACK packets, transmit falsified gateway beacons to repeatedly wake up sensors	sub GHz	Replay attacks, recovery of passwords, malicious message modification
ZWave	AES encryption with three shared keys	40 kbps	Mesh network	Does not enforce a standard key exchange protocol, Z-Wave devices implicitly trust the source and destination fields of 794 the MPDU frame	sub GHz	Key Reset, impersonation, node spoofing, Black Hole attacks
COAP	NoSec Shared Key -MultiKey- Certificate mode	250 Kbps	Tree topology	Proxies having to decide if DTLS implementation will be multi-cast or uni-cast message	56 MHz	Parsing, Cache, amplification, spoofing. Cross-protocol attacks
Wi-Fi	WPA2, SSID hiding, MAC filtering and static IP addressing, Connectivity issues over obstacles	0.1– 54 Mbps	Star	Lack of granular device authentication, weakness against denial of service, limited protection of service integrity	2.4 GHz, 5 GHz	DoS, Replay, Channel collision, Spoofing attacks
6LoWPAN	AES cipher suit, ESP, IKEv2, DTLS, connectivity issues over obstacles	50 kbps	Mesh topology	IP network, radio signal of implementations, Unchanged nodes address, fragmentation mechanism	2.4 GHz	Use of malicious intermediary network nodes, Signal jamming, traffic analysis
NFC	SSE, SCH, modes of operation: Read/Write, Peer-to-Peer	106– 424 Kbps	Point-to-p oint	Data exchange in close proximity, PICC emulations in protocol challenge-response requests	13.56 MHz	Near proximity, MITM, DoS, modification attacks.
HTTP	Basic-Digest authentication	1.15 Mbps	Bus topology	Data transfer is not encrypted		Evasedropping- theft- breach and manipulation, flooding attacks
ZigBee	128-bit AES with pre-share keys, frame protection mechanisms, essential key, global link key and unique link key	250 kbps	Mesh	Utilizing insecure key transportation for pre-shared keys, ACKs have no integrity checks, insufficient registration of network keys	2.4 GHz	Installing default link keys or sending security headers in clear text on auxiliary frames, looding that causes DoS, energy-consuming attacks
UWB	LRP/HRP secure ranging schemes, size of the UWB symbol	53– 480 Mbps	I. PEER TO PEER, MULTI-HOP	Long symbols length, wrong access control configuration or power failure	3.1–10.6 GHz	ED/LC, Same-Nonce attack
IrDA (Infrared)	No embedded security controls	14.4 Kbps	Point-to-p oint	Detect reflected infrared-light and filtering out the surrounding ambient noise	850–900 nm	Eavesdrop attack
WIA-PA	Join-key shared between device and security manager	250 Kbps	Mesh topology, Star topology	Lack of public key encryption algorithm, no intrusion prevention, no broadcast key, The first request is not encrypted	2.4 GHz	Sybil, DoS, wormhole, Jaming , traffic analysis attack
mDNS	mDNS packets on the network doesn't mean in any case a security risk, use firewall, antivirus, use always secure protocols if available (SSL, SSH, etc)	54Mb ps	Star topology	To obtain information about remote host (operating system type & exact version, MAC address , its hostname, and the list of services running.)		Spoofing Services, Man in the Middle Attacks, Denial of Service, Flooding
HL7	No built-in security	128 Kbps	Peer to peer	Message sources are often not validated by default, size of HL7 messages is often not validated	2.4GHz	Spoofing or integrity attacks, Flooding attacks
MQTT	Four-way handshake mechanism	1 mps	Star topology	No embedded data encryption mechanism, IP broker		Traffic analysis, Port Obscurity, Botnet Over MQTT
XMPP	Authenticated with Simple Authentication and Security Layer (SASL) and encrypted with Transport Layer Security (TLS)	28 Kbps	Mesh topology	Cisco meeting server software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition for users of XMPP	32 MHz	Sniffing Passwords, Breaking passwords through dictionary attacks, privilege escalation attacks

7. Why Favorite Target for Cyber Attackers in Healthcare Sector

Over the last few years, the healthcare industry has seen an increase in cyber threats. Protecting patients' electronic health records from various dangers has become a hot topic among medical professionals. However, with new dangers emerging every day, it's impossible to tell where an organization's budget should be spent. The healthcare sector is presently the most targeted for internet attacks for nine reasons [119], including a high demand for patient information and often-outdated systems. The number of healthcare equipment vulnerable to hackers is growing, posing a threat not only to people but also to entire networks. The following are some of the primary reasons why healthcare is one of the most vulnerable sectors to cyber-attacks.

7.1 Confidential Patient Data is Worth a Lot of Money

A staggering amount of patient data is stored at hospitals. They keep a large number of medical records, social security numbers, credit card information, and other personal information. The sector is becoming a growing target due of the secret data that is worth a lot of money to hackers who can easily sell it. According to IBM Security's annual study, the average cost of a data breach in 2020 was $3.86 million across all worldwide businesses, with healthcare having the highest industry-average cost of $7.13 million. Every company has a legal obligation to safeguard their patients' personal information. They may end up paying a lot of money on ransomware assaults if their systems aren't protected. The threat of ransomware is quite serious, especially for small businesses that may not have the financial resources to deal with cyber-attacks.

7.2 Medical Devices are an Easy Entry Point for Attackers

The large number of connected medical equipment, each with its own set of requirements and manufactured by different companies, makes security upkeep particularly difficult for healthcare IT specialists. There aren't many drawbacks to healthcare technology advancements these days. In today's healthcare, medical technologies such as x-rays, insulin pumps, and defibrillators are essential. These new devices, however, provide more entry points for attacks for those in charge of online security and patient data protection. Although the devices themselves may not contain the patient data sought by attackers, they can be utilised to initiate an assault on a server that does [120]. Unfortunately, many hospitals have so many gadgets that security is impossible to maintain. They are in charge of enormous amounts of information. Hackers could gain access to all of their networks. In the worst-case scenario, hackers might gain control of medical equipment, prohibiting healthcare organisations from giving life-saving therapy to patients. Medical gadgets do not hold any patient data, which hackers are well aware of. They regard them as an easy target, though, because they lack the security present on other network devices such as laptops and desktops. Medical device threats can pose issues for healthcare organisations by allowing hackers access to other network equipment or allowing them to install expensive ransomware. Keeping network equipment as secure as feasible helps to control the damage that a medical device attack could cause.

7.3 Members of Staff Need to Access Data Remotely More Opportunities for Attackers

Expectations are high in the healthcare industry. There are instances when employees need to access information from afar. This creates new opportunities for hackers to take advantage of. Remotely connecting to devices is risky since their devices are not always secure. Staff workers are not usually trained to deal with cyber security concerns or secure their devices. Unfortunately, hackers have turned their attention to healthcare data. They are after it because of its great worth, ease of access, and lack of adequate security measures. Because many health facilities now have to deal with significant amounts of data, the COVID 19 pandemic poses a heightened level of risk. They may be unable to establish adequate cyber security due to a lack of time or strategies. Risk-based authentication is one option for companies with employees that operate on several devices (RBA). This technology simplifies risk analysis by allowing IT employees to create policies that identify a device's risk depending on characteristics such as the user, their location, and more. Any odd activity is then notified, ensuring that critical patient information is never exposed to potentially dangerous equipment.

7.4 Unsecured Mobile Devices

When it comes to healthcare facilities that enable mobile logins, security rules aren't always enforced. Because all of the organization's planning and security do not affect employee communication devices, this leaves its networks exposed to malware and hackers. When staff disposes of equipment in order to improve the network, network information or passwords may still be available, providing a natural entry point for crooks. Employers have little power unless the firm establishes strong standards or outright prohibits user devices.

7.5 Healthcare Staff aren’t Educated in Online Risks

Medical experts are prepared to deal with a wide range of situations, but internet risks are not on their radar. Due to budget, resource, and time restrictions, all healthcare personnel cannot be fluent in cyber security best practises. Although cyber security solutions are complicated, their user interface must be straightforward [120]. Medical personnel want a secure network that is both quick and simple to use. They also require the assurance that patient data is secure so that they may concentrate on their work. MFA and SSO are gaining popularity because they simply use a secure one-time code to add extra layers of security without requiring the user to know anything other than their own login credentials.

7.6 Lost and Stolen Mobile Devices

In the same way, lost or stolen electronics pose a significant risk. When a mobile device needed to access a facility's network is lost or stolen, it becomes a liability. If it slips into the wrong hands, the user can quickly gain access to the system by utilising old or saved login information. It can be difficult to detect a criminal's presence or reseal the hole once they have gained access to the network.

7.7 Healthcare information Open and Shareable

Staff must have access to confidential patient data on many devices, both on-site and remotely. Because the medical sector is so fast-paced, employees need to be able to transmit information quickly; there's no time to think about the security implications of the devices they're using. IT professionals are concerned that the devices used to share information are not always secure. They can't constantly be available to check every device's credentials, especially in a time-sensitive situation. Users that need remote access to data will only need privileges for the tasks they need to complete. They won't require full admin account access if they're just checking their emails. Precautions like these reduce the likelihood of admin accounts being hacked. Multi-factor authentication (MFA) solutions prevent attacks from compromised credentials or unauthorised users, ensuring that only the proper individuals have access to important information.

7.8 Unrestricted Access to Computers

Unauthorized personnel can readily access computers that aren't in restricted places. Unauthorized workers or others in the region could swiftly obtain devastating information if these open PCs are connected to sensitive patient information. In other circumstances, successful phishing attempts on machines with public access provide a mechanism for hackers to gain access to more sensitive network regions. Make sure that any computer that stores patient data is kept in a secure area.

7.9 Third Parties (Vendors, Contractors, Partners)

Third-party personnel, such as suppliers and contractors, pose a significant danger to businesses, with the majority of them without a secure system or specialised team to manage them. Organizations are becoming increasingly conscious of the potential threat posed by third parties as cyber criminals become more adept and cyber security concerns continue to climb. RiskManagementMonitor.com published a report titled "Security Risks of Third-Party Vendor Relationships," which includes an info graphic estimating that 60 present of data breaches involve a third party, and only 52 present of companies have security standards in place for third-party vendors and contractors.

7.10 Small Level Healthcare Center are Also at Risk

Online threats pose a concern to all healthcare facilities. Large businesses retain the most data, giving the greatest reward for attackers and making them regular targets. Smaller healthcare facilities, on the other hand, have lower security costs. Smaller businesses are typically considered as an easy target, as well as a backdoor-access chance to target larger firms, due to less complicated and up-to-date cyber security systems. Because they are all in charge of sensitive patient data, effective cyber security solutions have become a necessary for all sizes of healthcare organisations. Healthcare executives are increasingly conscious of the need to increase spending on cyber security, and there are numerous solutions available that are scalable to various business sizes. MFA solutions add extra levels of security to your devices, preventing attackers from collecting login information by combining user passwords and one-time information that is unique to your firm.

7.11 Inadequate Disposal of Old Hardware

It's easy to imagine that once you've destroyed data, you don't have to worry about it being accessed by others. However, when users incorrectly dispose of hard drives, obsolete terminals, and other hardware used to access a network with EHRs or credentials, criminals have easy access to such information. It is possible to recover data even after drives have been wiped or reformatted, implying that everything the user saved is still vulnerable.

7.12 Outdated Technology Used in Healthcare Industry

Despite recent remarkable breakthroughs in medical technology, not every element of the healthcare business has followed up. Due to limited finances and a reluctance to learn new methods, most medical technology has become obsolete. The healthcare business continues to rely on antiquated, legacy systems. According to the research, 82 present of healthcare firms use Windows, with 76 present running Windows 7. Hospitals that use systems that still release system updates should ensure that all software is up to date. Bug patches are frequently included in these to keep systems secure. However, software will ultimately reach the end of its useful life, and producers will stop releasing updates. It is feasible to reduce the danger of cyber assaults by adding extra layers of security where it is not viable to change to new, more secure software or where medical professionals just do not want the hassle. To keep their patient data secure, healthcare organisations must respond to the latest cyber dangers. It's critical to set aside money and invest in the correct solution for your company. Consider how your employees prefer to work and stay on top of new risks as they surface before your systems become obsolete and you find yourself unable to safeguard all of your devices.

8. Possible Countermeasures for Security Threats in Medical Internet of Things (MIoT)

Medical Things can assist health care practitioners give more precise therapies for patients by providing a steady stream of real-time data through the Medical Internet of Things (MIoT). We require IoMT security for two reasons. The first is the issue of patient privacy. Medical data breaches might be humiliating and perhaps fatal for a patient. Another reason for MIoT security is to ensure the safety of patients. In many circumstances, the proper operation of a MIoT device could mean the difference between life and death for a patient. Fortunately, vulnerabilities in healthcare computer systems may be minimized. All data should be encrypted so that third parties cannot access it while it is being transmitted or stored. The basic message is that the security of MIoT devices is critical. It necessitates adequate device design as well as a secure method to keep them safe. There are a variety of methods for securing MIoT systems.

8.1 Token Based Security

Token-based authentication is a technique that allows users to prove their identity and obtain a one-of-a-kind access token in exchange [121]. Traditional password-based or server-based authentication solutions are not the same as token-based authentication. Tokens provide an additional degree of protection, and administrators have complete control over every activity and transaction. These tokens, such as IoT Ubidots [122], are used by cloud data analytics

businesses to protect the connection between the cloud layer and the nodes in the MIoT sensor and gateway levels. In a hospital information system, RFID can be employed as a hardware token for safe sensor logistic management. Tokens in this code language are small and can be passed quickly between two entities. You can control who has access to what, how long that access lasts, and what they may do while signed in.

8.2 Understand Your Network Map

Network mapping is a visual representation of your network and all of the devices that are linked to it. Many network performance monitors (NPMs) include a facility for creating or viewing network maps. Make use of technologies that gives you a bird's-eye view of your network's devices and storage. You'll be able to see exactly what data is vulnerable in which ways, and you'll be alerted when new or unapproved devices join the system. This structure will also assist you in determining the access and limitations for each device on the network, reducing inappropriate employee behavior. These maps show you how your network's devices are operating in easy-to-understand images.

8.3 Hierarchical Access Control

Cryptographic procedures can be used to enforce hierarchical access control policies, in which users and objects are linked to nodes in a hierarchy. This method allows patients' data on the cloud layer to be accessed in a hierarchical manner. This method employs a hierarchical role-based model, with authorization granted based on the user's role [123]. The technology offers a simple hierarchical security strategy that encrypts the data of the patients and only decrypts the data that the user is authorized to see. Hierarchical access control is a key mechanism for authorizing data or other resources access privileges. It has a wide range of applications, including computer science, electronics, [124], and automation.

8.4 Update Our Software

Make certain that all software and operating system information is current. These updates include essential patches that deter potential thieves from exploiting previously discovered software flaws. Criminals can still take advantage of the weaknesses created by previous versions if you do not use the required software updates. You may ignore those software update warnings, but you'll be missing out on a lot, starting with your cyber security.

8.5 Gait-Based Technique

Wearable healthcare devices are collecting and storing an increasing amount of sensitive personal information, including physical, physiological, and daily activities, making device security critical. Gait-based identity identification is a new technology that is increasingly being employed for wearable device access control due to its high performance. Sun et al. [125] created a symmetric key in just 10 gait cycles utilizing a set of MIoT sensors mounted to the individual's body. They claim that their system can create three times the number of bits each gait cycle as comparable state-of-the-art systems. This technology uses an artificial neural network [126] model to generate 13 bits every gait cycle, resulting in a 128-bit key in just ten minutes. This key can be used to protect communications between MIoT sensors and an AP or mobile device [127] in the future gateway layer.

8.6 Virtual Private Network Encryption

You may need to access essential files on your healthcare network if you operate remotely. This type of data necessitates a secure connection for security reasons. Encrypting your network connection is an excellent technique to protect your network and keep hackers out. A Virtual Private Network (VPN) encrypts your data so that others can't see what your computer sends or receives. So, even if they were watching your connection, unless they already had access to your computer, they would not receive anything. A VPN's principal function is to conceal your IP address from your ISP and other third parties. This allows you to communicate and receive information over the internet without fear of being intercepted by anyone other than you and your VPN provider. To limit the risk of data leakage, VPN services connect to private servers and use encryption methods.

8.7 Facial Recognition

Face recognition is a technique for recognizing or validating an individual's identification by looking at their face. Face recognition software can identify persons in photographs, videos, or in real time. Face scanning can be used to authenticate users in IoT systems. Biometric security includes facial recognition. Facial recognition can be utilized as a second factor in continuous role-based authentication by leveraging shared keys as a first factor [128]. This keeps the gateway layer communication between the sensor and the medical controller safe and dependent on the privileges of each authorized user. Face recognition algorithms are meant to calculate a probability match score between the unknown individual and specific face templates contained in the database, rather than positively identifying an unknown person [129]. Instead of returning a single result, these algorithms will present numerous probable matches, sorted in order of likelihood of right identification. For example, in the absence of a higher privileged medical staff who has authenticated him/her but has not logged out of the system, this strategy can prevent lower-level medical staff from accessing the patient's data.

8.8 Conduct Regular Audits

Regular audits should be conducted by system administrators, and two-step authentication should be in place, requiring anyone wishing to change information or enter new data to prove their identity. All users should be obliged to set secure passwords and update them when a certain amount of time has passed. Access credentials should be checked on a regular basis to verify that no former or transferred personnel have access to patient information. Most employers benefit from safety audits and inspections since they have been proved to lower the number of incidents. Rather than waiting for an accident to happen, we encourage being proactive about safety.

8.9 Elliptic Curve Cryptography (ECC) With Cryptographic Hash Function (CHF)

Elliptic Curve Cryptography (ECC) is a key-based data encryption technology. For decryption and encryption of web traffic, ECC focuses on pairs of public and private keys. ECC is a sophisticated cryptography technology that is an

alternative to RSA. It uses the mathematics of elliptic curves to generate security between key pairs for public key encryption [130]. In simple cyber security terms, a cryptographic hash function (CHF) is a computer algorithm that assists in authenticating users and securing their data against any breach by those attempting to get access through hacking or other immoral means. It authenticates future access by using system-generated encrypted data specific to each user input data and detecting a match in the user input data. The ECC feature, in combination with CHF keys, can be utilised to create a secure certificate-free channel between patients and their physicians [131]. The goal behind combining the ECC and the CHF is to provide a secure method of sharing keys between the key generation server in the cloud layer and the nodes in the MIoT sensor and gateway layers. The size of IoMT data is significant, and it is growing. The patient's data can be safely exchanged among the system's entities by separating it into subsets and transforming it using ECC keys and CHF. Clear text passwords are converted to enciphered text for storage using a cryptographic hash function (CHF). If an attacker wants to exploit your database, they'll have to decipher those hash values. In other words, hashes make attackers take longer [132]. A crypto system based on elliptic curve cryptography (ECC) requires much less memory. With increasing security measures, the ratio rapidly rises. For example, an RSA crypto system with a 1024-bit key length is equivalent to an elliptic curve crypto system with a 163-bit key length.

8.10 Set Strict Access

Consider the following facts instead of focusing simply on what you need to restrict. What resources do certain personnel require in order to do their duties? This creates an environment in which only the bare minimum of information is available, reducing the risk of staff misuse.

8.11 Homomorphic Encryption

Traditional encryption systems are not totally secure from an intermediary service like cloud servers due to sensitive data privacy breaches. Homomorphic encryption is a type of encryption that can be used to tackle security and privacy challenges. It allows you or a third party (such as a cloud provider) to perform operations on encrypted data without revealing the data's values [133]. This method secures the privacy of the patient's data by storing it as cypher text in the cloud layer and using it to perform mathematical operations like data integrity. A homomorphic cryptosystem is similar to other types of public encryption in that it encrypts data with a public key and only allows the person with the matching private key to view the decrypted data. In other words, this is ideal for some MIoT sensors, such as a smart watch, because it allows the data to be encrypted at all times and only seen by the patient, with the exception of emergencies, when the patient's data can be provided to medical staff to make proper diagnoses. Homomorphic encryption techniques perform best when data is represented as integers and the operational functions are addition and multiplication. This means that the encrypted data can be manipulated and studied just like plaintext data without having to decode it. To put it another way, HE can let your workers (or a third party) to work with and use encrypted data without knowing or having access to the decrypted data [134]. The healthcare industry may achieve a greater level of data security with homomorphic encryption without disrupting business processes or application functionality. This industry can maintain data privacy while yet extracting intelligence from sensitive data [135]. Cloud workload protection, aggregate, information supply chain consolidation, and automation and orchestration are all examples of how homomorphic encryption is used (operating and triggering off of encrypted data for machine-to-machine communication).

8.12 Think like a Hacker

You'll be far better able to thwart a cybercriminal's efforts if you understand the basics of how they exploit a network. While without a background in healthcare data security procedures, it may be impossible to account for this, this critical stage will identify any potential weaknesses in our approach. As a result, security professionals must always think like an opponent, or "think like a hacker."

8.13 Digital Signatures

A mathematical system for proving the validity of digital messages or documents is known as a digital signature. It is a virtual fingerprint that is unique to each individual and is used to identify signers and protect data in digital documents [136]. It is a sort of electronic signature that ensures legal compliance by verifying the validity and authenticity of a digital document as well as the identity of the signer. Even a tiny IoMT system can benefit from digital signature techniques. Public-key cryptography is used to create digital signatures. Public key cryptography is a type of encryption that employs a private and public key pair mechanism. Only the signer has access to the private key, which encrypts the contents. The recipient receives the public key, which decrypts the data in the digital document. To connect the signer and their signature, both parties must have a registered digital certificate from an issuing certificate authority. The document's security, accuracy, and validity are all ensured by public key cryptography. With an add-on software shim, digital signatures can be embedded into the sensor's firmware, intercepting and validating the sensor's wireless connections in MIoT systems [137]. With digital signatures, businesses may save money and time by signing documents and contracts with a single click of a button. There are significant cost and time savings, especially when the person who must sign is located in a distant geographical area. The risk of document duplication or manipulation is reduced with digital signatures. Signatures are checked, authenticated, and legitimate using digital signatures.

8.14 Use Professional Services

Though there are various approaches for health organizations to prevent possible threats, your expertise is in using data to aid patients, not in managing data security in healthcare. You can get expert network security and support by delegating network security to a specialized outside organization, allowing your team to focus more directly on medical-related responsibilities.

8.15 Light Based Systems

Li-Fi (Light Fidelity) uses Visible Light Communication (VLC) technology to provide wireless data transmission that is up to 100 times quicker than Wi-Fi. Solid-state illumination (SSL), such as LED bulbs, is used [138]. It is less prone to interference, and Li-Fi can travel through salty saltwater in the same way as light can. Because Li-Fi does not use wireless communications, it does not interfere with the hospital network and has a large free operation frequency as well as a narrow coverage range for increased security [139].

Because radio waves can flow through walls, they can be intercepted by persons outside your network, jeopardising the security of your data. Li-Fi, on the other hand, is more secure than Wi-Fi since light can be prevented by opaque surfaces. Some rooms can also be designated as high-security zones with their own Wi-Fi networks.

8.16 Consider Cloud Migration for Our Medical Data

For healthcare data storage and backup, the cloud provides a secure and adaptable alternative. It also allows for on-demand scaling of resources, which can significantly improve the way healthcare firms manage their data. Even if there is a breach or disruption, cloud-based backup and disaster recovery solutions ensure that patient records are available. These technologies, when combined with the ability to regulate data access, can provide the necessary level of security.

8.17 Blockchain in MIoT

Blockchain is a method of storing data in such a way that it is difficult or impossible to alter, hack, or cheat it. A Blockchain is a digital log of transactions that is duplicated and spread across the Blockchain full network of computer systems [140]. Each block on the chain contains a number of transactions, and whenever a new transaction occurs on the Blockchain, a record of that transaction is added to the ledger of each participant. Distributed Ledger Technology is a decentralised database that is administered by various people (DLT). Blockchain is a sort of distributed ledger technology in which transactions are recorded using a hash, which is an immutable cryptographic signature. In MIoT systems, Blockchain technology is commonly employed as a security management sharing tool for data between patients and other parties such as doctors and insurance companies [141]. Given the data quantities and connectivity needs in MIoT systems, Blockchain technology may suffer from latency, storage difficulties, and communications overhead. Due to its dispersed nature and decentralisation, public Blockchain technology has a high latency. As a result, private Blockchain could be used in real-time applications [142]. Hackers would have to change every block in the chain, across all distributed versions of the chain, if they intended to destroy a Blockchain system.

8.18 The 5G Role

5G is the next generation of wireless technology, and it's especially well-suited to device-to-device communication. With higher Internet speeds, lower latency, virtual networks, and a larger number of linked MIoT devices, 5G appears to be the next big upheaval in healthcare. It facilitates remote patient monitoring and expands access to healthcare without the risks of travel, expenses, and time that already exist. Advances in technology will reduce the time it takes to download large amounts of patient data and improve the quality of telemedicine by eliminating video delays and buffering. Robotic operations with augmented reality/virtual reality (AR/VR) will aid in greater competence and precision, hence improving care quality.

8.19 Patch Management

For a number of reasons, not all MIoT devices can be patched. Patching your MIoT devices can eliminate the system's vulnerabilities for those who can. When you set up a patch management procedure, make a note of any vulnerable devices that can't be fixed and make sure the rest of your MIoT devices are patched properly to avoid the most recent risks.

8.20 Enforce a Cloud Driven Network

Healthcare organizations should consider moving to a cloud-based network to effectively accommodate all IoMT devices. The latest cloud technologies promise to revolutionize how companies manage their networks, allowing them to move beyond basic network administration and into realms of real-time innovation and insight. To accommodate ever-increasing connectivity demands, they provide enhanced availability, flexibility, and reduced operational complexity. A cloud-based network is a sensible method for forward-thinking healthcare facilities to significantly simplify, protect, and future-proof their operations.

9. Technical Inadequacy

Technology businesses all over the world are substantially investing in the research and development of technologies that will aid in the digital transformation of the healthcare industry and expedite patient care techniques. By facilitating effective collaboration between healthcare personnel, patients, processes, and medical equipment, MIoT aids in the fundamental transformation of the healthcare sector. The technology opens up new treatment options, enhances and streamlines remote medical assistance, and allows for the collection of vital real-time data on a patient's health status. To provide best-in-class patient care, medical facilities now rely on Medical Internet of Things (MIoT) technologies. The Medical Internet of Things is poised to change the way the healthcare business operates. By offering visibility into the field, the Internet of Things is enhancing the sensory capacities of its products. There are many different types of MIoT devices on the market today. However, there may be several hurdles that healthcare organizations encounter while creating and integrating these devices into existing healthcare systems. In this section, we'll go over a few technological shortcomings that must be solved in order to fully fulfill the promise of Medical Internet of Things systems through digital transformation.

9.1 Quality of Service

Many Internet-based health-related applications demand high service quality. Health organizations cannot rely on the Internet for crucial tasks unless they have assurances that data will be delivered swiftly and accurately to its intended destination. For example, if video-based telemedicine is to become practical, care professionals must be able to rapidly and reliably retrieve medical records when they are needed for patient care; providers and patients must be able to secure sustained access to high-bandwidth services for remote consultations. Because clinicians may need rapid access to huge medical information and photos from different sources connected to the Internet, both bandwidth and latency may be crucial issues in emergency care settings.

9.2 Data Processing

The processing and analysis of data is a big difficulty in the healthcare business. The vast volume of data that hospitals, clinics, and health professionals collect contributes to the problem. It is difficult for companies to provide better and more tailored care to patients without sophisticated AI

systems that can analyse this data. Another significant problem is data collection and synchronisation. Doctor visits are taking place across various channels as a result of the rise of telemedicine, making it more difficult for health professionals to maintain patients' health information. As a result, the healthcare industry will need to develop a system for recording and updating health information for both in-person and virtual visits. Furthermore, legislation such as the EU's General Data Protection Regulation (GDPR) imposes significant restrictions on how businesses gather, utilise, and keep personal data. Fines under the GDPR can be as high as €20 million, or 4% of a company's annual sales. Therefore, it is in the best interest for all organizations to respect and follow all of GDPR requirements.

9.3 Multicast

Multicast contrasts with today's unicast delivery model, in which users communicate one-on-one, and the broadcast model of radio and television, in which a single transmitter broadcasts information to a vast number of unnamed consumers. Multicast enables large-scale multiparty conferencing while maximising network capacity use. It also allows for the efficient dissemination of streaming media to a large number of recipients at the same time. Multicast, on the other hand, introduces significant issues in terms of appropriate pricing methods and strategies to protect ISP networks from potential misuse. A related trend is the development of reliable multicast, which aims to enable the reliable transport of data from a single source to a large number of recipients, even if the network has periodic packet loss. Multicast applications in health care may place a greater emphasis on design and implementation aspects than applications in other sectors.

9.4 Coexistence

With billions of devices, radio channel congestion is an issue that is only going to become worse. Standards bodies have created test procedures to evaluate device functioning in the presence of other signals in order to alleviate wireless congestion. In Bluetooth, for example, adaptive frequency hopping (AFH) allows a Bluetooth device to discard channels with a lot of data conflicts. Listen before speak (LBT) and cooperative collision avoidance (CCA) are two further collision avoidance approaches that improve transmission efficacy. However, the effectiveness in a mixed-signal environment is unknown, and collisions and data losses will occur if the radio formats do not identify each other. A medical infusion pump that stops working owing to environmental interference, or an industrial sensor that loses its control signal, can have disastrous repercussions. Coexistence testing is also essential for determining how a device will perform in a congested, mixed signal environment, as well as the risk of maintaining wireless performance in the presence of unwanted signals present in the same operational environment.

9.5 Securities

For Internet-based health applications, security is a significant consideration. When personal health information is transmitted over the Internet or stored on a network-connected device, precautions must be taken to ensure that the information is (1) accessible to those who need it, (2) protected from those who do not have the proper credentials, and (3) not altered, either intentionally or unintentionally, in violation of established policies and procedures. Most Internet-based health care applications, whether they involve the transfer of personal medical records between health care providers or between a provider and a plan administrator, video telemedicine consultations, data reporting in a home monitoring situation, or the use of remote equipment in a biomedicine experiment, are concerned with these three requirements.

9.6 Connectivity

Because wireless communication is highly complex, and dense device deployments further complicate operations, enabling a seamless flow of information to and from a device, infrastructure, cloud, and applications is a top IoT problem. Even in the harshest settings, mission-critical IoT devices are expected to perform consistently and without fail. Fast-changing wireless standards add to the complication, and engineers are always challenged to stay up with the latest technology while ensuring that devices function together seamlessly across the ecosystem. Responding to connection difficulties necessitates the creation of extremely flexible and adjustable design and testing solutions that can be upgraded to meet future needs.

9.7 Broadband in Healthcare

Before the health community and consumers of health care can benefit from future Internet applications, they must have enough bandwidth in their local connections to ISPs to accommodate the expected traffic loads. Health-care organizations, for example, will need Internet connections capable of sending hundreds of kilobits per second, if not megabits per second, to send comprehensive radiographic images to faraway specialists for near-real-time analysis. High-bandwidth connections will be required by biomedical research institutes undertaking distributed simulations. Many of these requirements will be met by leasing communications lines with sufficient capacity. Conversely, some firms who deliver material through the Internet and anticipate strong demand for their services may try to offload parts of their activities to third parties that can provide the necessary capacity, though this model may have drawbacks in health applications.

9.8 Digital User Experience

Last but not least, creating flawless and user-friendly products such as a connected heart monitor, mobile application, or any other digital product or service is a huge issue. When it comes to any type of technology, the end user must be considered in order to create a user-friendly product or service. This is critical in the healthcare industry because many items will be used by both patients and medical professionals. A patient's experience with an uncomfortable or badly designed MIoT device, for example, can be tainted, causing them to remove the device, reducing the data it can collect. On the other hand, if a MIoT device's software is difficult to use, it will limit medical professionals' willingness to utilise or prescribe the device to other patients. The lack of standards, particularly when it comes to MIoT, makes it more difficult for these goods and services to work flawlessly in a connected device ecosystem. Nonetheless, technology's ability to make significant changes in the healthcare industry will be primarily determined by its overall quality.

9.9 Continuity

One of the most essential aspects for IoT devices is ensuring and prolonging battery life. In consumer IoT devices, a long battery life is a big competitive advantage. The industry standard for industrial IoT devices is a battery life of five to ten years. Device life can represent the difference between life and death for medical devices like pacemakers. Of course, a dead battery isn't an option. Integrated circuit (IC) designers must create ICs with deep sleep modes that consume very little current and reduce clock speed and instruction sets, as well as implement on low battery voltages, to meet IoT battery life requirements. Standards groups are defining new low power consumption operating modes for wireless communications, such as NB-IoT, LTE-M, LoRa, and Sigfox, which enable restricted active operation time while consuming minimal power. Designers who include sensing, processing, control, and communication components into a finished product must understand how peripherals behave and consume power, as well as optimise the product's firmware and software to simplify operation and reduce consumption.

9.10 Protected Web Browsing

Because e-mail forwarding does not necessitate a real-time link between sender and receiver, it is relatively simple to safeguard sender anonymity, at least in part. Web browsing is more difficult to secure since it relies on a relatively quick connection between client and server. Even if the message contents and addresses are disguised, the timing of message arrival and departure may make it evident to an observer that two parties are interacting. The problem of concealing a user's identity from a server that it accesses can be divided into two parts: first, how to prevent an eavesdropper from tracing the path of the traffic; and second, how to prevent the server from sending traffic over the path that causes the client to reveal information that could identify the user (against the user's wishes). The majority of the mechanisms established to safeguard Web browsing have been, or could be, applied to support anonymous e-mail and other services (for example, file sharing, news, and VPNs).

10. Challenges of Security and Privacy in MIoT

We need to figure out how to handle the data load safely as the number of linked devices grows. The safety of a patient's medical, insurance, and personal information must be prioritized. Because most MIoT devices were not developed with security in mind, they are particularly vulnerable to hacking. Because threats and vulnerabilities cannot be removed, lowering cyber security risks is particularly difficult. Manufacturers, hospitals, and facilities must collaborate to handle cyber security concerns in the health-care ecosystem, which is complicated. Because of the black market value of electronic health records, which can be worth hundreds or even thousands of dollars, cybercriminals usually target them. Securing medical devices necessitates dealing with a variety of dangers that are typical in the MIoT. Several difficulties must be addressed in order to develop a better security environment.

10.1Critical Nature of Medical Devices

Medical devices include highly personal information that offers specific hazards to medical device end users and organisations that support medical devices if it falls into the wrong hands.

10.2 Insecure Network

A number of devices and software services rely heavily on wireless networks, such as Wi-Fi, because of their convenience and low cost. However, wireless networks are known to be vulnerable to various intrusions, including unauthorized router access, man-in-the-middle attacks, spoofing, and denial of service attacks, brute-force attacks, and traffic injections. Furthermore, the majority of uncertified free Wi-Fi networks in public places are untrustworthy [143].

10.3 Security is not Prioritized

Because the majority of patients and healthcare professionals who use medical devices are not IT experts, device manufacturers place a premium on ease of use. Devices designed and manufactured with strict security standards are typically cumbersome or difficult to use for healthcare practitioners or end-users, which means that security is often a low priority for device manufacturers.

10.4 Data Remanence and Freshness

The residual representation of data that has been officially deleted or destroyed is referred to as data remanence. Data remanence may result in an inadvertent breach of data confidentiality. Data confidentiality and integrity are insufficient in the healthcare system [144] if data freshness is not taken into account. The term “data freshness” refers to the need for current and accurate patient health records. Data inconsistency is caused by storage delays and transmitting out of date messages, especially in critical situations.

10.5 Lightweight Protocols for Devices

To deliver services, low-cost devices and software applications based on sensors should adhere to specified policy and proxy requirements. At the moment, we must use high-cost solutions if we want to provide high-grade security for sensors. In the MIoT system, there is a conflict. The key objective of security protection in the future will be to develop multiple degrees of security protocols based on application circumstances, particularly lightweight security protocols.

10.6 Security Patches and Upgrades are Difficult to implement

Medical equipment, unlike ordinary IT devices, sometimes lack built-in mechanisms for updating their [145] software when a security patch or upgrade is available. When medical equipment is assigned to a patient, they cannot be taken down for patching.

10.7 Data Sharing

Despite the rapid advancement of medical information technology, the Information Island phenomenon is becoming more significant. The standards of data collected [146] from different manufacturers' devices varies greatly, making management difficult to unify. Information collaboration and sharing among heterogeneous MIoT systems, on the other hand, is an unavoidable future trend. The security of the MIoT system could be jeopardised if patient information is privatized. With hierarchical security architecture, using generic data policies to mix various data could deliver more

comprehensible information while also improving security and privacy.

10.8 Network Segmentation

Segmentation is essential for implementing a good security plan. Splitting a network into subnets is a common technique for companies to increase performance and medical IoT security. You can separate traffic into external (guests and external users) and internal (internal users) segments using network segmentation (authorized users). Without it, a locally implemented device could have a severe influence on the entire business when it comes to moving sensitive medical data. A hacker can simply take control of misconfigurations within an organisation without network segmentation. Look for additional access on any server or workstation connected to an internal network, for example.

10.9 Mass Production of Medical Devices

Medical equipment is mass-produced on a vast scale, with just the most minimum testing and inspection performed prior to shipment. This raises the possibility of a security breach as a result of a flaw.

10.10 Detecting Attacks is Difficult

The sheer number and variety of MIoT devices makes them not only challenging to manage, but also to monitor. Many other IT systems, including different networks, clouds, and apps, can be connected to MIoT devices. Companies are scrambling to fulfil the increased demands for monitoring as the number of connected devices continues to expand. Vulnerabilities and breaches might go undiscovered without good and constant cyber surveillance.

10.11 Long Life Devices

Some medical gadgets are used for months or even years at a time. Because of this, attackers have a large window of opportunity to conduct assaults against devices. It also increases the likelihood that a known security issue may be discovered during the deployment of a device, making it easy to penetrate the device if it is not modified to remedy the flaw.

10.12 Data Eavesdropping

In most cases, only authorised caregivers have access to a patient's health information [147]. However, data transmitted over wireless networks can be intercepted. For example, a widely used IoT-based glucose monitoring and insulin administration system makes use of wireless communication links, which are commonly used to launch privacy assaults, necessitating adequate data protection.

10.13 User Deployed Devices

Patients or healthcare providers who set up medical devices on their own may be unaware of or fail to follow security best practises such as changing the device's default access settings.

10.14 Energy Optimization

Sensors are important components of healthcare systems. With the advancement of sensor technology, it is now much easier to collect measurable and analysable healthcare data. Wearable devices have become increasingly common in healthcare systems in recent years. Wearable technologies have the potential to capture a lot of healthcare data without bothering patients [148]. However, energy consumption is a significant issue with wearable gadgets. Wearable gadgets are small devices that capture data from people's bodies. They continuously collect healthcare data from the body [149]. To capture and deliver health data to healthcare applications, a battery is insufficient. Furthermore, wearable device batteries must be charged on a regular basis. These are significant issues for IoT devices in healthcare.

10.15 End Users Cannot Observe the Health of the Device

Medical devices often provide little or no opportunity for patients and healthcare providers to check the device's status. Medical gadgets, unlike regular computers, do not allow users to log in to view status information or see who has accessed the device.

10.16 Device Communication

Communication is one of the most difficult aspects of establishing smart or connected health. Many devices now have sensors for data collection, and they frequently communicate with the server in their own [150] language. Because each manufacturer has its own proprietary protocol, sensors from different manufacturers may or may not be able to communicate with one another.
Because of the fragmented software environment and privacy issues, valuable information is frequently isolated on data islands.

11. CONCLUSION

The ageing of the population has presented new difficulties to society and healthcare. A few years ago, patient monitoring was limited to the care of family members or home nurses if the patient was recovering at home. If, on the other hand, a patient chooses to be admitted to the hospital, regular monitoring is a must. However, as time passes and IoT health monitoring tools grow more common, the option of recuperating from home becomes more appealing. Patients do not need to be beneath the hospital's roof because of the integration of real-time monitoring and other specific modules. The Medical Internet of Things (MIoT) is a network of implantable or wearable medical devices that collect medical data on a patient's health status on a continuous basis. Medical gadgets with Wi-Fi that allow machine-to-machine communication are among them. Though the Internet of Things has enhanced operations and patient care, it has also raised the amount of vulnerabilities. Because medical devices are either vulnerable or unprotected from potential attackers. As a result, any cyber-attack could have devastating effects, putting patients' lives in jeopardy, preventing the widespread adoption of MIoT. Because cyber security hazards to medical devices are always developing, premarket safeguards alone will not be able to entirely address them. Every sector faces cyber security challenges, and the health-care industry is no exception. Cyber dangers, which can be incredibly costly, require organisations to be exceedingly watchful. In this paper, we will identify the main threats that may compromise the security of MIoT devices and systems, as well as the security and privacy requirements, characteristics of cyber-attacks in MIoT, Protocol Security Weaknesses, and the necessary and appropriate measures that are required for MIoT security. Finally, this study identifies

open and upcoming research areas in future Medical Internet of Things (MIoT) systems that must be addressed.

12. The Future of Medical Internet of Things (MIoT)

Because of its potential to improve patient participation and health-care delivery, the Medical Internet of Things (MIoT) is expected to grow at an exponential rate in the future. While the disruptive innovation of MIoT is exciting on one side, security issues are significant on the other. The issues are only going to get more difficult as the market for Medical Internet of Things grows. Healthcare organisations will face a hurdle in storing mountains of data acquired by numerous devices. Because this data will be shared with other devices, security concerns will arise. Unauthorized access to linked equipment can jeopardise the safety of the patient. As a result, proper authentication and authorisation will be required to succeed with MIoT. The applications that MIoT has to offer are still in the early stages of development. The use of connected devices in the healthcare system is also unsatisfactory. IoT and healthcare, when combined, will drastically alter hospital service offerings. The Medical Internet of Things will bring digitization to healthcare. Because there is no time to waste when it comes to patient care.

REFERENCES

[1] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. ,"Internet of Things (IoT): A vision, architectural elements and future directions", Future Gener. Comput. Syst., 29, pp. 1645–1660, 2013

[2] Yusuf Perwej, Mahmoud Ahmed AbouGhaly, Bedine Kerim and Hani Ali Mahmoud Harb. "An Extended Review on Internet of Things (IoT) and its Promising Applications", f Communications on Applied Electronics (CAE), New York, USA, Volume 9, Number 26, Pages 8 – 22, February 2019, DOI: 10.5120/cae2019652812

[3] Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.: The Internet of Things for health care: a comprehensive survey. IEEE Access 3, 678–708, 2015

[4] Yusuf Perwej, Majzoob K. Omer, Osama E. Sheta, Hani Ali M. Harb, Mohmed S. Adrees, "The Future of Internet of Things (IoT) and Its Empowering Technology" , International Journal of Engineering Science and Computing (IJESC), Volume 9, Issue No.3, Pages 20192 – 20203, March 2019

[5] Stellios, I.; Kotzanikolaou, P.; M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor, 20, 3453–3495, 2018

[6] Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, "An Empirical Analysis of Web of Things (WoT)", International Journal of Advanced Research in Computer Science, Volume 10, No. 3, Pages 32-40, 2019, DOI: 10.26483/ijarcs.v10i3.6434

[7] Yusuf Perwej, Faiyaz Ahamad, Mohammad Zunnun Khan, Nikhat Akhtar, "An Empirical Study on the Current State of Internet of Multimedia Things (IoMT)", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), ISSN (Online) 2394-2320, Volume 8, Issue 3, Pages 25 - 42, March 2021 DOI: 10.1617/vol8/iss3/pid85026

[8] A. Pantelopoulos and N. G Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis", IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.), vol. 40, no. 1, pp. 1-12, 2010

[9] Nikhat Akhtar, Saima Rahman, Halima Sadia, Yusuf Perwej, "A Holistic Analysis of Medical Internet of Things (MIoT)", Journal of Information and Computational Science (JOICS), ISSN: 1548 - 7741, Volume 11, Issue 4, Pages 209 - 222, April 2021 DOI:10.12733/JICS.2021/V11I3.535569.31023

[10] Yusuf Perwej , Firoj Parwej, "A Neuroplasticity (Brain Plasticity) Approach to Use in Artificial Neural Network", the International Journal of Scientific & Engineering Research (IJSER), France , ISSN 2229 – 5518, Volume 3, Issue 6, Pages 1- 9, June 2012 DOI: 10.13140/2.1.1693.2808

[11] Yusuf Perwej, "An Experiential Study of the Big Data", International Transaction of Electrical and Computer Engineers System (ITECES), USA, Science and Education Publishing, Volume 4, No. 1, Pages 14-25, March 2017 DOI: 10.12691/iteces-4-1-3

[12] Y. Jin, "Low-cost and active control of radiation of wearable medical health device for wireless body area network", J. Med. Syst., vol. 43, no. 5, pp. 137, 2019

[13] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in 2014 IEEE International Conference on Industrial Engineering and Engineering Management, 2014, pp. 1244–1248

[14] Q. Jing, A. V., J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and Challenges," Wirel Netw, vol. 20, no. 8, pp. 2481–2501, 2014

[15] Stellios, I.; Kotzanikolaou, P., M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor, 20, 3453–3495, 2018

[16] Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, "A Perusal of Big Data Classification and Hadoop Technology", International Transaction of Electrical and Computer Engineers System (ITECES), USA, Volume 4, No. 1, Pages 26-38, May 2017, DOI: 10.12691/iteces-4-1-4

[17] J. Tang, A. Liu, M. Zhao, and T. Wang, "An aggregate signature based trust routing for data gathering in sensor networks," Security and Communication Networks, Vol. 2018, 30 pages, 2018

[18] Yusuf Perwej, S. A. Hannan, Firoj Parwej, Nikhat Akhtar ,"A Posteriori Perusal of Mobile Computing", International Journal of Computer Applications Technology and Research, ATS (Association of Technology and Science), Vol. 3, Issue 9, pp. 569 - 578, 2014, DOI: 10.7753/IJCATR0309.1008

[19] Bai Yan, Yao Lingsheng, Wei Tao, Tian Fei, Jin Dong-Yan, Chen Lijuan, et al., Presumed Asymptomatic Carrier Transmission of COVID-19. JAMA, vol. 323, no. 14, pp. 1406-1407, 2020

[20] Dang, L.M.; Piran, M.J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 2019, 8, 768.

[21] Nikhat Akhtar, Yusuf Perwej, "The Internet of Nano Things (IoNT) Existing State and Future Prospects", GSC Advanced Research and Reviews (GSCARR), Volume 5, Issue 2, Pages 131-150, 2020, DOI: 10.30574/gscarr.2020.5.2.0110

[22] Bilcke, J., Beutels, P., Brisson, M., Jit, M.: Accounting for methodological, structural, and parameter uncertainty in decision-analytic models: a practical guide. Med. Decis. Making 31(4), 675–692 (2011)

[23] Dang LM, Piran M, Han D, Min K, Moon H.,"A survey on internet of things and cloud computing for healthcare", . Electronics 8(7):768, 2019

[24] Park, K., Pak, J.: An integrated gateway for various phds in healthcare environments. BioMed. Res. Int., 2012

[25] Jia, Pengfei, and Jia Yan. "Classification of Wound Infection Data Based On SVM with A Novel Weighted Gaussian RBF Kernel." International Journal of Hybrid Information Technology, vol.9.10, pp. 201-210, 2016
[26] Qi, J., Yang, P., Min, G., O., Dong, F., Xu, L.: Advanced internet of things for personalised healthcare systems: a survey. Pervasive Mob. Comput. 41, 132–149, 2017
[27] O. Diggelmann and M. N. Cleis, "How the Right to Privacy Became a Human Right," Human Rights Law Review, vol. 14, pp. 441–458, 07 2014
[28] Fabian, B., Ermakova, T., Junghanns, P.: Collaborative and secure sharing of healthcare data in multi-clouds. Inform. Syst. 48, 132–150, 2015
[29] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. Journal of Network and Computer Applications, 84:25–37, 2017
[30] J. L. Kernec, F. Fioranelli, S. Yang, J. Lorandel, and O. Romain, "Radar for assisted living in the context of internet of things for health and beyond," in Proceedings of the IFIP/IEEE International Conference on Very Large Scale Integration (VLSISoC), pp. 163–167, Verona, Italy, October 2018
[31] Yusuf Perwej, Firoj Parwej, Mumdouh Mirghani Mohamed Hassan, Nikhat Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review", International Journal of Scientific Research in Computer Science Engineering and Information Technology, Volume 5, Issue 1, Pages 462-482, 2019, DOI: 10.32628/CSEIT195193
[32] A.Mawgoud, Ahmed et al. "Cyber Security Risks In MENA Region: Threats, Challenges and Countermeasures". Springer, Cham, International Conference On Advanced Intelligent Systems and Informatics, 2019, pp. 912-921
[33] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," Future Generation Computer Systems, vol. 55, pp. 266–277, 2016
[34] Sumanta Kuila, Namrata Dhanda, Subhankar Joardar, Sarmistha Neogy, and Jayanta Kuila. A generic survey on medical big data analysis using internet of things. In First International Conf. on Artificial Intelligence and Cognitive Computing, pages 265–276. Springer, 2019
[35] Yusuf Perwej , Kashiful Haq, Firoj Parwej, M. M. Mohamed Hassan," Internet of Things (IoT) and its Application Domains", International Journal of Computer Applications, Vol. 182, No.49, Pp 36- 49, April 2019 , DOI: 10.5120/ijca2019918763
[36] Anna Challoner and Gheorghe H Popescu. Intelligent sensing technology, smart healthcare services, and internet of medical things-based diagnosis. American Journal of Medical Research, 6(1):13–18, 2019
[37] Yusuf Perwej, Bedine Kerim, Mohmed Sirelkhtem Adrees, Osama E. Sheta, "An Empirical Exploration of the Yarn in Big Data", International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, New York, USA, Volume 12 , No.9, Pages 19-29 , 2017, DOI: 10.5120/ijais2017451730
[38] Rithesh, R. N. "SVM-KNN: A Novel Approach to Classification Based On SVM and KNN." International Research Journal of Computer Science 4.8, 2017
[39] Yusuf Perwej , "Recurrent Neural Network Method in Arabic Words Recognition System", International Journal of Computer Science and Telecommunications (IJCST), which is published by Sysbase Solution (Ltd), UK, London, (http://www.ijcst.org) , ISSN 2047-3338, Volume 3, Issue 11, Pages 43-48, November 2012
[40] L. H. Iwaya, Engineering Privacy for Mobile Health Data Collection Systems in the Primary Care. PhD thesis, Karlstads universitet, 2019
[41] H. Turabieh, A. Abu Salem, and N. Abu-El-Rub, "Dynamic L-RNN recovery of missing data in IoMT applications," Future Generation Computer Systems, vol. 89, pp. 575–583, 2018
[42] Yusuf Perwej, "An Evaluation of Deep Learning Miniature Concerning in Soft Computing", International Journal of Advanced Research in Computer and Comm. Engineering, Vol. 4, Issue 2, PP 10 - 16, 2015, DOI: 10.17148/IJARCCE.2015.4203
[43] S. Brooks, M. Garcia, N. Lefkovitz, S., and E. Nadeau, "Nistir 8062 an introduction to privacy engineering and risk management in federal systems," 2017
[44] Premarathne, U.S.: Hybrid cryptographic access control for cloud based electronic health records systems. IEEE Cloud Comput. 2, 1–7, 2017
[45] Yusuf Perwej, Firoj Parwej, Asif Perwej," Copyright protection of digital images using robust watermarking based on joint dlt and dwt", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, pp.1--9, 2012
[46] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," in Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms, and Programming, PAAP '15, pp. 217–222, December 2015
[47] Esposito, C., de Santis, A., G., et al.: Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5(1), 31–37, 2018
[48] Grammatikis PIR, Sarigiannidis PG, Moscholios ID.. Securing the internet of things: challenges, threats and solutions. Internet of Things 5(7), pp.41–70, 2019
[49] Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, October, 2018
[50] Khatoon, A. ,"A Blockchain based smart contract system for healthcare management", Elect. 9, 94, 2020
[51] Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security", International Journal of Recent Scientific Research (IJRSR), Vol. 9, Iss. 11, (A), PP, 29472 – 29493, 2018, DOI: 10.24327/ijrsr.2018.0911.2869
[52] Dr. Yusuf Perwej, Prof. (Dr.) Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security", International Journal of Scientific Research and Management (IJSRM), ISSN (e): 2321-3418, Volume 9, Issue 12, Pages 669 - 710, December 2021 DOI: 10.18535/ijsrm/v9i12.ec04
[53] Alsubaei, F., Abuhussein, A., & Shiva, S. ," Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment", In Local Computer Networks Workshops (LCN Workshops), 2017 IEEE 42nd Conference on , IEEE, pp. 112-120, 2017
[54] A. D. Stern, W. J. Gordon, A. B. Landman, and D. B. Kramer, "Cybersecurity features of digital medical devices: An analysis of FDA product summaries", BMJ Open, vol. 9, no. 6, 2019
[55] M. Huang, A. Liu, T.Wang, C. Huang, "Green data gathering under delay differentiated services constraint for internet of things," Wireless Communications and Mobile Computing, vol. 2018, 2018

[56] H. Huang, J. Zhou, W. Li, J. Zhang, X. Zhang, G. Hou, ``Wearable indoor localisation approach in Internet of Things," IET Netw., vol. 5, no. 5, pp. 122_126, 2016
[57] R. Saeedi, J. Purath, K. Venkatasubramanian, and H. Ghasemzadeh, "Toward seamless wearable sensing: Automatic on-body sensor localization for physical activity monitoring," in Proc. 36th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., pp. 5385-5388, 2014
[58] T S Khatri and G B Jethava, "Survey on data Integrity Approaches used in the Cloud Computing", International Journal of Engineering Research & Technology, vol. 1, no. 9, November 2012
[59] Yusuf Perwej, Bedine Kerim, Mohmed Sirelkhtem Adrees, Osama E. Sheta, "An Empirical Exploration of the Yarn in Big Data", International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, New York, USA, Volume 12 , No.9, Pages 19-29 , December 2017, DOI: 10.5120/ijais2017451730
[60] T. Nilges, ``The cryptographic strength of tamper-proof hardware," Karlsruhe Inst. Technol., Karlsruhe, Germany, Tech. Rep. urn:nbn:de:swb:90-518099, 2015
[61] Brodnik, M., L. Rinehart-Thompson and R. Reynolds ," Fundamentals of Law for Health Informatics and Information Management Professionals", Chicago: AHIMA Press., Chapter 1, 2012
[62] P. Crilly and V. Muthukkumarasamy, "Using smart phones and body sensors to deliver pervasive mobile personal healthcare", in Proc. 6th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process., pp. 291-296, 2010
[63] McWay, Dana.,"Legal and Ethical Aspects of Health Information", Third Edition. New York: Cengage Learning, Chapter 9, 2010
[64] A. Kogetsu, S. Ogishima, and K. Kato, "Authentication of patients and participants in health inform. exchange and consent for medical research: A key step for privacy protection, respect for autonomy, and trustworthiness," Frontiers Genet., vol. 9, p. 167, Jun. 2018
[65] Yusuf Perwej ," The Hadoop Security in Big Data: A Technological Viewpoint and Analysis", International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE) , Volume 7, Issue 3, Pages 1-14, 2019, DOI: 10.26438/ijsrcse/v7i3.1014
[66] FDA. "FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps". Press Announcement, 2019
[67] Yusuf Perwej, Md. Husamuddin, Fokrul Alom Mazarbhuiya,"An Extensive Investigate the MapReduce Technology", International Journal of Computer Sciences and Engineering (IJCSE), E-ISSN : 2347-2693, Volume-5, Issue-10, Page No. 218-225, Oct-2017, DOI: 10.26438/ijcse/v5i10.218225
[68] Y. Lu, L. D. Xu, "Internet of things cybersecurity research: A review of current research topics", IEEE IoT Jou., vol. 6, no. 2, pp. 2103-2115, 2019
[69] Yusuf Perwej, Md. Husamuddin, Majzoob K.Omer, Bedine Kerim, "A Comprehend the Apache Flink in Big Data Environments" , IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, P-ISSN: 2278-8727, USA, Volume 20, Issue 1, Ver. IV, Pages 48-58, Feb. 2018, DOI: 10.9790/0661-2001044858
[70] M. Hayashi, M. Owari, G. Kato and N. Cai, "Secrecy and robustness for active attack in secure network coding", Proc. IEEE Int. Symp. Inf. Theory (ISIT), pp. 1172-1177, Jun. 2017
[71] Nikhat Akhtar, Nazia Tabassum, Asif Perwej, Yusuf Perwej, " Data Analytics and Visualization Using Tableau Utilitarian for COVID-19 (Coronavirus)", Global Journal of Engineering and Technology Advances (GJETA), Volume 3, Issue 2, Pages 28-50, 2020, DOI: 10.30574/gjeta.2020.3.2.0029
[72] F. S. Tsai and K. L. Chan, "Detecting Cyber Security Threats in Weblogs Using Probabilistic Models", pp. 46-57, 2007
[73] R. Sabillon, J. Cano, V. Cavaller and J. Serra, "Cybercrime and Cybercriminals: A Comprehensive Study", Intl. Journal of Computer Networks & Comm. Security, vol. 4, no. 6, pp. 165-176, 2016
[74] D. Steinmetzer, J. Chen, J. Classen, E. Knightly and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves", Proc. IEEE Conf. Commun. Netw. Secur. (CNS), pp. 335-343, Sep. 2015
[75] Sarah Spiekermann. Ethical IT innovation: A value-based system design approach. Auerbach Publications, 2015
[76] Danesh Irani, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu. Reverse social engineering attacks in online social networks. In International conference on detection of intrusions and malware, and vulnerability assessment, pages 55–74. Springer, 2011
[77] L. Ma, "Detecting masqueraders in 802.11 wireless networks", Proc. Int. Wir. Netw, pp. 267-271, 2011
[78] N. Vidgren, K. Haataja, and P. Toivanen, "Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned," Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 5132–5138, 2013
[79] 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
[80] 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
[81] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," International Conference on Pervasive Computing: Advance Communication Technology and Appl. for Society, ICPC, vol. 00, no. c, pp. 0–5, 2015
[82] Alejandro Proano and Loukas Lazos,"Selective jamming attacks in wireless networks", In 2010 IEEE International Conference on Communications, pages 1–6. IEEE, 2010
[83] O. Zheng, J. Poon, and K. Beznosov, "Application-Based TCP Hijacking," 2009
[84] 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
[85] S. Jucker, "Master's Thesis Securing the Constrained Application Protocol by Stefan Jucker," no. October, pp. 1–103, 2012
[86] Yuquan Shan, George Kesidis, Daniel Fleck, and Angelos Stavrou. "Preliminary study of fission defenses against low-volume dos attacks on proxied multiserver systems", 12th International Conference on Malicious and Unwanted Software, pages 67–74, IEEE, 2017
[87] Meecham Andy, Tim Acker, "Underwater threat detection and tracking using multiple sensors and advanced processing", Security Technology (ICCST) IEEE International Carnahan Con. on, IEEE, 2016
[88] Yusuf Perwej, Kashiful Haq, U. Jaleel , S. Saxena , "Some Drastic Improvements Found in the Analysis of Routing Protocol for the Bluetooth Technology Using

Scatternet", Special Issue on the International Conference on Computing, Communications and Information Technology Applications (CCITA-2010), Ubiquitous Computing and Communication Journal (UBICC), Seoul, South Korea, ISSN Online: 1992-8424, ISSN Print: 1994-4608, Volume CCITA-2010, Number 5 , Pages 86-95, 2010

[89] N. BeNazir, I. Minar, and M. Tarique, "BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY," International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, 2012

[90] Junghyun Nam, Juryon Paik, H-K Kang, Ung Mo Kim, and Dongho Won. An off-line dictionary attack on a simple three-party key exchange protocol. IEEE Communications Letters, 13(3):205–207, 2009

[91] Ruhma Tahir, Huosheng Hu, Dongbing Gu, Klaus McDonald-Maier, and Gareth Howells. Resilience against brute force and rainbow table attacks using strong icmetrics session key pairs. In Communications, Signal Processing, and their Applications (ICCSPA), 1st International Conference on, pages 1–6. IEEE, 2013

[92] Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the Internet of Things. IEEE Commun. Surv. Tutor, 21(2), pp.1636-1675, 2019

[93] Younghwa Lee and Kenneth A Kozar. Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM, 48(8):72–77, 2005

[94] Yusuf Perwej, "A Literature Review of the Human Body as a Communication Medium using RedTacton", Communications on Applied Electronics (CAE), Foundation of Computer Science FCS, USA, Vol. 9, No.4, PP 7 – 17, 2016, DOI: 10.5120/cae2016652161

[95] Ibrar Yaqoob, Ejaz Ahmed, Muhammad Habib ur Rehman, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Ali Al-garadi, Muhammad Imran, and Mohsen Guizani. The rise of ransomware and emerging security challenges in the internet of things. Computer Networks, 129:444–458, 2017

[96] 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, Feb 2017

[97] Georgios Kambourakis, Constantinos Kolias, and Angelos Stavrou. The mirai botnet and the iot zombie armies. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM), pages 267–272. IEEE, 2017

[98] A. Mohsen Nia, N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Comp., vol. PP, no. 99, p. d, 2016

[99] A. Cui et al., "When Firmware Modifications Attack: A Case Study of Embedded Exploitation", NDSS The Internet Society, 2013

[100] Mendez, D.M.; Papapanagiotou, I.; Yang, B. Internet of things: Survey on security and privacy. arXiv 2017

[101] Fouladi, B.; Ghanoun, S.-SensePost UK Honey, i'm home!!, hacking zwave home automation systems. Black Hat USA, Las Vegas, Nevada; 2013

[102] Hummen, R.; HillerShafagh, H. Wehrle, K. 6LoWPAN fragmentation attacks and mitigation mechanisms. In Proceedings of the 6th ACM Conference on S: ecurity and Privacy inWireless and Mobile Networks, WiSec, Budapest, Hungary, pp. 55–66, 2013

[103] Alghamdi, T.A. Lasebae, A. Aiash, M. Security Analysis of the Constrained Application Protocol in the Internet of Things. In Proceedings of the Second International Conference on Future Generation Communication Technologies (FGCT 2013), London, UK, 12–14 pp. 163–168, 2013

[104] Sundaresan, S.; Doss, R.; Zhou, W. RFID in Healthcare–Current Trends and the Future. In Mobile Health; Springer: Berlin/Heidelberg, Germany, pp. 839–870, 2015

[105] Rahman, R.A.; Shah, B. Security analysis of IoT protocols: A focus in CoAP. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016, Muscat, Oman, 15–16, pp. 172–178, 2016

[106] Singh, M.; Leu, P.; Capkun, S. UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. In Proceedings of the 26th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 24–27, 2019

[107] Haataja, K.M.J. Box, P.O. Kuopio, F. "Security in Bluetooth, WLAN and IrDA: A comparison Department of Computer Science Security", University of Kuopio: Kuopio, Finland, pp. 1–14, 2006

[108] Fan, X.; Susan, F.; Long,W.; Li, S. Security Analysis of Zigbee; Computer Network Security Class, Massachusetts Institute Tech.Cambridge, 2017

[109] Ferreira, R.; Aguiar, R. Breaching ,"location privacy in XMPP based messaging", IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 , pp. 917–922, 2012

[110] Haselsteiner, E.; Breitfuß, K. Security in Near Field Communication (NFC) Strengths and Weaknesses. Semiconductors, 11, 71, 2006

[111] Qi, Y.; Li, W.; Luo, X.; Wang, Q. Security analysis of WIA-PA protocol. In Advanced Technologies in Ad Hoc and Sensor Networks; Springer: Berlin/Heidelberg, Germany, pp. 287–298, 2014

[112] LeCroy. CATC Merlin II—Bluetooth V1.2 Protocol Analyzer; LeCroy: Santa Clara, CA, USA, 2003

[113] Dinculeanˇa, D. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Appl. Sci. , 9, 848, 2019

[114] Andy, S.; Rahardjo, B.; Ha, B. ,"Attack scenarios and security analysis of MQTT communication protocol in IoT system,"4th International Conference on Electrical Engineering, Computer Science and Informatics, Yogyakarta, Indonesia, 19–21,; pp. 1–6, 2017

[115] Cheshire, S.; Krochmal, M. DNS-Based Service Discovery. Available online: https://tools.ietf.org/html/rfc6763 (accessed on 15 March 2021)

[116] Nixon, M. A Comparison of WirelessHART™ and ISA100.11a. In Emerson White Paper; Emerson Process Management: St. Louis, MO, USA, pp. 1–36, 2012

[117] Zhang, X.;Wei, M.;Wang, P.; Kim, Y. Research and implementation of security mechanism in ISA100.11a networks. In Proceedings of the 2009 9th International Conference on Electronic Measurement Instruments, Beijing, China, 16–19, pp. 4-716–4-721, 2009

[118] Moustis, D.; Kotzanikolaou, P. Evaluating security controls against HTTP-based DDoS attacks. In Proceedings of the IISA, Piraeus, Greece, 10–12 July 2013; IEEE: pp. 1–13, 2013

[119] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis", Big Data Anal., vol. 1, pp. 6, 2016

[120] Y. Xu, D. Tran, Y. Tian, and H. Alemzadeh, ``Poster abstract: Analysis of cyber-security vulnerabilities of interconnected medical devices," presented at the

IEEE/ACM Int. Conf. Connect. Health, Appl. Syst. Eng.Technol. (CHASE), Sep. 2019

[121] L. Xiong, D. Peng, T. Peng, H. Liang and Z. Liu, "A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks", Sensors, vol. 17, no. 11, pp. 2681:1-28, 2017

[122] Ubidots. "IoT and Cloud tools to build your business."[Online]. Available:https://ubidots.com [Accessed: 18- Nov-2020].

[123] T. Belkhouja, S. Sorour, and M. S. Hefeida, "Role-Based Hierarchical Medical Data Encryption for Implantable Medical Devices," IEEE Global Comm. Conference (GLOBECOM), 9-13, pp. 1-6, 2019

[124] Tolone, W., G.J. Ahn, T. Pai and T. "Access control in collaborative systems",. ACM Comput. Surv., 37: 29-41, 2005

[125] Y. Sun and B. Lo, "An Artificial Neural Network Framework for Gait-Based Biometrics," IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 3, pp. 987-998, 2019

[126] Yusuf Perwej, "The Bidirectional Long-Short-Term Memory Neural Network based Word Retrieval for Arabic Documents", Transactions on Machine Learning and Artificial Intelligence (TMLAI), Society for Science and Education, United Kingdom (UK), Volume 3, Issue 1, Pages 16 - 27, 2015, DOI: 10.14738/tmlai.31.863

[127] Bobick, A.F., Johnson, A.Y.: Gait recognition using static, activity-specific parameters. In: Proceedings of IEEE Computer Vision and Pattern Recognition Conference, pp. 423–430, Kauai, Hawaii, 2001

[128] V. H. Tutari, B. Das, and D. R. Chowdhury, "A Continuous Role-Based Authentication Scheme and Data Transmission Protocol for Implantable Medical Devices," in 2019 Second International Conference on Advanced Computational and Communication Paradigms *(ICACCP)*, 25-28, pp. 1-6, 2019

[129] Z. Cao, Q. Yin, X. Tang and J. Sun, "Face recognition with learning-based descriptor", Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 2707-2714, Jun. 2010

[130] Koblitz, N., Menezes, A., Vanstone, S.: The State of Elliptic Curve Cryptography. In: "Towards a Quarter-Century of Public Key Cryptography", Kluwer Academic Publishers, pp. 173–193, Boston (2000)

[131] P. Kasyoka, M. Kimwele, and S. Mbandu Angolo, Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system," Journal of Medical Engineering & Technology, vol. 44, no. 1, pp. 12-19, 2020

[132] P. Rogaway, and T. Shrimpton, "Cryptographic Hash- Function Basics: Definitions, implications and separations for preimage resistance, second preimage resistance, and collision resistance", inFSE, 2004, pp.371-388

[133] J.H. Cheon, A. Kim, M. Kim and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers", International Conference on the Theory and Application of Cryptology and Information Security, pp. 409-437, 2017

[134] Z. Brakerski, C. Gentry and V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping", ITCS'12 Proceedings of the 3rd Innovations in Theoretical Com. Science Conf., pp. 309-325, 2012

[135] Yusuf Perwej, "The Hadoop Security in Big Data: A Technological Viewpoint and Analysis", International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE) , Volume 7, Issue 3, Pages 1-14, 2019, DOI: 10.26438/ijsrcse/v7i3.1014

[136] J. Feghhi and P. Williams, Digital Certificates: Applied Internet Security, MA, Reading: Addison-Wesley, 1999

[137] C. Easttom and N. Mei, "Mitigating Implanted Medical Device Cybersecurity Risks," in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0145-0148, 2019

[138] Yusuf Perwej, "The Next Generation of Wireless Communication Using Li-Fi (Light Fidelity) Technology", Journal of Computer Networks (JCN), USA, Science and Education Publishing, Volume 4, No. 1, Pages 20-29, 2017, DOI: 10.12691/jcn-4-1-3

[139] A. Mosaif and S. Rakrak, "A Li-Fi based wireless system for surveillance in hospitals," Biomedical Spectroscopy and Imaging, vol. 8, pp. 81-92, 2019

[140] Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications", Open Science Journal of Electrical and Electronic Engineering (OSJEEE), New York, USA, Volume 5, No. 4, Pages 30 - 43, 2018

[141] X. Chen, H. Zhu, D. Geng, W. Liu, R. Yang, and S. Li,"Merging RFID and Blockchain Technologies to Accelerate Big Data Medical Research Based on Physiological Signals," Journal of Healthcare Engineering, vol. 2020, pp. 1-17, 2020.

[142] Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security", International Journal of Recent Scientific Research (IJRSR), Vol. 9, Issue 11, (A), PP. 29472 – 29493, 2018, DOI: 10.24327/ijrsr.2018.0911.2869

[143] H. Zhang, Z. Cai, Q. Liu et al., "A survey on security-aware measurement in SDN," Security and Communication Network, vol. 2018

[144] Yusuf Perwej, Mohammed Y. Alzahrani , F. A. Mazarbhuiya, Md. Husamuddin, "The State of the Art Cardiac Illness Prediction Using Novel Data Mining Technique", International Journal of Engineering Sciences & Research Technology, Volume 7, Issue 2, Pages 725-739, 2018, DOI: 10.5281/zenodo.1184068

[145] A. Arbaugh, "A Patch in Nine Saves Time?," in IEEE Security and Privacy. Vol. 37, pp. 82-83, 2004

[146] Yusuf Perwej**,** Firoj Parwej, Nikhat Akhtar, "An Intelligent Cardiac Ailment Prediction Using Efficient ROCK Algorithm and K- Means & C4.5 Algorithm", European Journal of Engineering Research and Science (EJERS), Bruxelles, Belgium, Vol. 3, No. 12, Pages 126 – 134, 2018, DOI: 10.24018/ejers.2018.3.12.989

[147] J. Xu and B. Chen, "Secure coding over networks against noncooperative eavesdropping", IEEE Transactions on Information Theory, vol. 59, no. 7, pp. 4498-4509, July 2013

[148] A. Rodríguez, A. Ordóñez and A. Ordóñez, "Energy consumption optimization for sensor networks in the IoT", IEEE Colombian Conference on Communications and Computing, 2015

[149] J.C. Kwan and A.O. Fapojuwo, "Radio Frequency Energy Harvesting and Data Rate Optimization in Wireless Information and Power Transfer Sensor Networks", IEEE Sensors Journal, vol. 17, no. 15, pp. 4862-4874, 2017

[150] K. Doppler, M. Rinne, C. Wijting, C. Ribeiro and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks", IEEE Commun. Mag., vol. 47, no. 12, pp. 42-49, 2009