1. Medical IoT: Opportunities, Issues in Security and Privacy – A Comprehensive Review

Deepa Krishnan and Swapnil Singh

https://orcid.org/0000-0002-6236-0955 and https://orcid.org/0000-0002-1422-9549

Abstract

Health care IoT industry has witnessed tremendous momentum in recent years due to the widespread availability of high-speed internet and multi-functional cost economical sensors of varying sizes ranging even to nano sizes. The medical community and end-users have embraced the potential of IoT in leveraging cost-effective medical care like never before. The adoption of innovative technology has been steadily increasing over the years, be it consumer devices, wearable devices, and in-body devices.

However, most device manufacturers overlook the security and privacy aspect of the devices in the rat race to deliver the devices to the market. A successful compromise of a wearable IoT device can further escalate security attacks on other parts of health care networks as distributed denial of service attacks (DDoS). In recent years we have witnessed few alarming cases where patient safety and the confidentiality of their data was at stake. This underscores the growing necessity of adopting the best security practices in medical IoT.

In the proposed book chapter, we have reviewed the growing importance of IoT in the medical field and few important use-cases that have caught our attention. The recent security attacks targeting smart health care and security and privacy concerns are comprehensively analysed. We have also surveyed the existing solutions for security and privacy concerns of medical IoT and have presented a critical review of challenges in existing mechanisms that can open further research in this area.

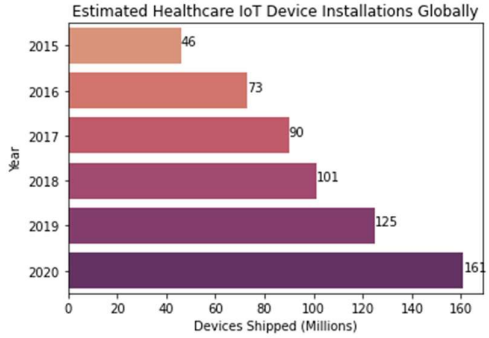
Keywords– Health care, Internet of Things, IoT, Privacy, Security.

1.1 Introduction

We are witnessing a world where a pandemic has severely limited the medical fraternity in operating at their full potential because disease management has to be administered remotely many a times. This introduces the need for increased technical support for the health care sector. Automating the diagnostic process can help reduce the load on hospitals and doctors and deliver timely medical care to the needy across the globe. With its far-reaching potential, the Internet of things is such a method of automation that can remarkably impact the health care industry. Medical IoT inherently consists of sensors that can record various body vitals like glucose level, blood pressure, pulse rate, heart rate, etc., and can be sent to cloud servers where data analytic and machine learning algorithms can deliver valuable insights.

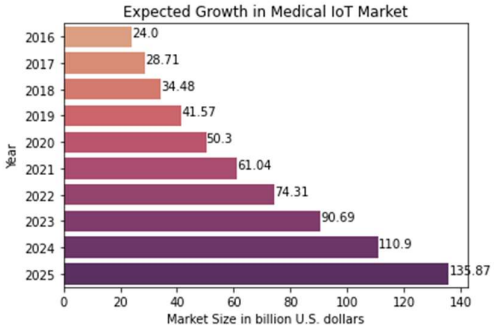
As stated earlier, the use of IoT has revolutionized the medical sector. Healthcare systems use IoT devices to create an infrastructure that monitors health parameters and automatically acts whenever medical intervention is required. (Tarouco et al. 2012). The IoT-based medical devices may be more economically beneficial in the long run. However, that is not the only reason for the increased adoption of IoT in the health care sector. The shortage of paramedics and doctors is likely to boost the adoption of IoT devices in the medical sector. It is expected that the USA alone will face a shortage of 125000 physicians by 2025, and this shortage is likely to be greater in Asia and Africa. According to BI Intelligence, around 161 million medical IoT devices have been in use since 2020; the trends of the expected number of Health IoT devices installed globally are shown in Figure 1.1. (Mordo intelligence

2021)As seen in Figure 1.2, the medical IoT market is expected to grow to 135.87 billion dollars by the year 2025 (Department 2016); IoT devices can be particularly useful where social distancing norms are being enforced to control the Covid-19 pandemic.



<Figure 1.1 here>

Figure 1.1. Expected Healthcare IoT Device installations globally (Mordo intelligence 2021)



<Figure 1.2 here>

Figure 1.2. Expected Growth in Medical IoT Market (Department 2016)

With the help of IoT, we can set up better and more efficient remote health monitoring systems; REMOA is one such project that targets home solutions for the health monitoring of patients with chronic illnesses. This system includes strategies and protocols for data transfer between different sensing devices like movement sensors and blood pressure monitors. All sensors are connected wirelessly to each other and the central monitor. The monitor is responsible for accommodating, aggregating, and comparing the collected information against series. When the limit is crossed, it can raise the alarm and trigger the health workers to react promptly to the health-related event. (Tarouco et al. 2012)

According to WHO, 17.9 million people die of cardiovascular disease every year. 4 out of 5 patients suffering from heart diseases die due to heart attacks and strokes. One-third of such deaths are premature in people below the age of 70. Regular monitoring and check-ups could reduce the risk of such diseases and help prevent strokes and heart attacks. However, regular monitoring inconveniences the patients greatly and might not even yield the data useful for medical prognosis or diagnosis. IoT-based monitoring devices mitigate these inconveniences and can be more efficient and reliable. Intelligent monitoring solutions can trigger emergency medical intervention when body vitals show anomalies. Smart health motoring is an amalgamation of intelligent computing in addition to remote health monitoring with IoT. The body sensors network constitutes various wearable or implantable devices like cardioverter-defibrillator and pacemakers, which can sense and monitor blood pressure, heart rate, and other such vitals of the body. These devices stack the data in a clinical dataset, which can later be referred (Sarmah 2020).

IoT is vigorously promoted in health care by all leading global health care institutions. Microsoft developed intelligent systems to formulate a structure to capture health data from IoT devices, thus ensuring the required connectivity. Intel aims to bring health care anytime and anywhere. It emphasizes

synchronizing health data streaming and communication systems in real-time to lower the cycle time and the first-time quality of many existing medial workflow environments. In collaboration with various well-known firms, IBM has developed IoT devices for a series of health care solutions like health analytics of healthcare data, data governance of health care data, and connected home health. Apple came up with the Apple Watch to monitor your blood oxygen levels, heart rate, and blood pressure. The Memorial Hermann healthcare system entirely relies on Apple's solution for providing connection and efficient healthcare, giving secure access, physician gains, and better care. Cisco is working with various health organizations to build a health-grade network architecture, deploy converged system-based networks, and provide algorithms to handle substantial incoming IoT data. Qualcomm developed an integrated solution that can capture and deliver real-time data from health devices to databases and portals. Indian Government took various initiatives to boost the use of IoT in the medical sector. Countries like the USA, Australia, Japan, France, Germany, China, and Korea have already taken various healthcare sector initiatives, and even the Indian Government has also started taking steps in this direction. (Darshan and Anandakumar 2016). We can see a growing influx of a wide variety of IoT devices used in the medical field.

There are different categories of medical IoT devices which are used in today's connected world. In the following section, we have described some important categories of IoT devices based on their utility.

1.1.1 Wearable IoT devices

If we categories IoT devices as per their application, we can do so as, i) IoT for Toddlers, ii) IoT for kids, iii) IoT for chronic care, iv) IoT for Motion Detection and body motion reconstruction, v) IoT for Personal Emergency response systems, vi) IoT for Surgery Guidance, and vii) IoT in mobility aids. Mimo, a resting device built to monitor respiration, sleeping position, and body temperature, then collects the data and sends it to the working parents; this is an example of IoT for Toddlers. Another such example is milk nany; this device makes warm baby milk using milk powder, all of this with a press of a button on the phone. TempTraq is a Bluetooth patch that tracks the baby's temperature and sends the data to the caretaker's mobile phone. This is also an example of IoT for Toddlers. Smart Diapers are another example of an IoT device for Toddlers; it is a thin sensor placed in the diaper which informs the caretaker that it is the time to change the diaper. (Yeole and Kalbande 2016)

iSwimband is an IoT device for kids; it is a Bluetooth-connected device; if the device is submerged for a user-defined time, it alerts the connected iOS device. Sleep monitoring systems are also an excellent example of the use of IoT devices for kids. These systems track the natural sleeping environment, body parameters like temperature, blood pressure, and movement while sleeping. IoT devices are also being used for chronic care; these can be implants or wearable devices. Wearable devices include temperature sensors and CO sensors to prevent breathing. (Yeole and Kalbande 2016)

Wearable motion trackers are used to monitoring body motion; the sensor is placed at rotational angles and lower extremity joints. The data collected from these sensors can be used for tumor detection. This system is activated in the ICU when we need to track the activities of the patient. Certain devices are used for personal emergency response. Blood pressure measurement sensors are one such example of these devices. Google glasses are used for a higher percentage of success in surgeries; google glasses help doctors to confirm their decision during surgery. Pathfinder wheelchairs and stretchers are very useful as mobility aids; these are IoT devices for finding a path. Gemalto has developed an automatic pill dispenser consisting of IoT, mobile phones, and wireless M2M. The pillbox is wirelessly connected to the patient, doctor, family member, and medical alert monitoring center. (Yeole and Kalbande 2016)

1.1.2 Implantable Medical Devices

Besides the patient monitoring devices, many IoT devices embedded in the human body could track and report body parameters. The recent advances in nanocircuits and manufacturing materials for in-body devices have propelled the growth and popularity of implantable devices. Implantable devices are placed in the human body through a medical procedure and left in the body. Some of these are even capable of regulating and alter vital statistics of the human body. For instance, some examples are

cardiac pacemakers, coronary stents, and implantable insulin pumps, to name a few. Cardiac Pacemakers are used in patients whose heart rhythm is prone to be very high or too low or impeded due to any heart trauma (American Heart Association editorial staff 2015). Another popular device is an insulin pump surgically inserted into the abdominal tissue and releases basal insulin via a catheter (Spaan et al. 2014). It is highly efficient than conventional wearable insulin because it is delivered to the peritoneal cavity and released in a controlled way to the body. The cardiac stents with a vast user base worldwide are popular among these implantable devices. They are used to improve the blood flow in blocked coronary arteries (Hoare et al. 2019)

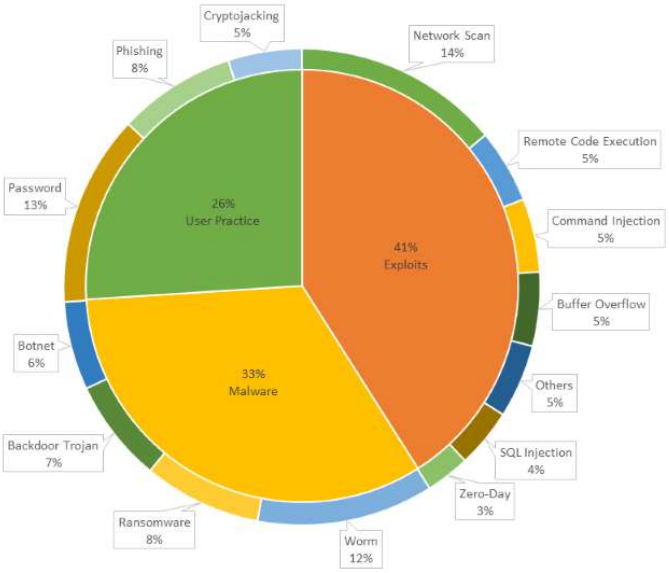
1.1.3 Stationary Medical IoT Devices

Stationary devices are used to measure physiological parameters, and the most commonly used are nuclear imaging devices, X-ray and mammography devices, ultrasound machines, CT, and MRI scanners. These are comparatively costly and sophisticated devices that transmit diagnostic images wirelessly to physicians and are generally used by hospitals and diagnostics centers. These images are collected and integrated into the patient's Electronic Health Record (EHR). Stationary medical devices help in timely diagnosis and are integrated with other knowledge management systems, this aids in quick and efficient decision-making. Most IoT devices use Wi-Fi, Bluetooth, and Zigbee technology to communicate with peer devices and the server. (Kodali, Swamy, and Lakshmi 2016) Besides, Near Field Communication (NFC) has also observed that cellular and satellite communication have also been used for end-to-end connectivity of remote patients with health care infrastructure.

The use of innovative technology in health care has been increasing in recent years, and this is further accelerated with the challenges thrown by the Covid-19 pandemic. The easiness with which consumers embraced smart health care will propel its usage further in the coming years. The proposed book chapter is organized as follows: Section 1.2 describes medical IoT security and privacy issues. Section 1.3 reviews the existing solutions for security and privacy issues in Medical IoT. Further, in Section 1.4, the challenges in existing solutions are given, finally, in Section 1.5, the conclusion and future scope of medical IoT devices' security and privacy issues.

1.2 Privacy and Security Issues in Medical IoT

We have discussed the potential applications of IoT in the medical sector in Section 1.1. As stated in the above section, IoT has several advantages, like being cost-friendly and remote monitoring. Along with these advantages, we have several problems and issues, raising concerns for using IoT in the medical sector. IoT devices in the medical field are deployed with minimal security features and are prone to attacks like denial of power attacks, eavesdropping, tampering parameter configurations, hijacking, device cloning, denial of service, and tampering messages. (Somasundaram and Thirugnanam 2020) Security attacks in IoT devices tend to cause damage, disrupt, misdirect, misuse, malfunction, or unauthorized access to the device. (Alraja, Farooque, and Khashab 2019)
In Figure 1.3, we can see that (O'Donnell 2020) 41% of the threats for IoT devices in healthcare are of exploit type, including Zero-Day, network scan, SQL injection, remote code execution, buffer overload, command injection, and others; 33% of the threats are due to Malware, including Botnet, Backdoor Trojan, Ransomware, and Worm, whereas the rest 26% is due to User practices line passwords, phishing, and crypto-jacking. As we observe, there are multiple threats to the security and the privacy of IoT devices in medical care and the patient; therefore, it is the need of the hour to identify these threats and provide solutions to tackle them. It is observed that device manufacturers ignore security aspects while producing IoT products and give more importance to the functionality of devices. One such example is that the IoT-based glucose monitoring and insulin delivery system frequently launches various security and privacy attacks. (AL-mawee 2012)



<Figure 1.3 here>
Figure 1.3. Frequently occurring cyber-attacks (O'Donnell 2020)

1.2.1 Security Issues in Medical IoT

The challenges posed by medical IoT devices, unlike other IoT installations, are multi-fold. The consequences are more significant as they can directly affect the health and life of users. In this section, the major categories of security attacks are described as follows:

1.2.1.1 Data Level

Security of medical data concerning confidentiality, integrity, and availability is very critical. The different categories of security attacks for medical data are as follows:

- Data Leakage
  Collecting and storing a patient's medical records must be done completely and ethically following the previously set norms. In case of such a data breach, cybercriminals can access it, and the data can be sold in illegal markets like the dark web. This would be a violation of privacy regulation and cause possible reputational damage and financial risks. (Sun, Lo, and Lo 2019) If the data for a political leader or an essential personality leaks similarly, this data can physically harm that person or even kill the person. The data's confidentiality needs to be preserved so that medical information cannot be leaked to an adversary. Eavesdropping is an attack where the intruder just enters the network and listens to the data being transmitted. Eavesdropping is also known as snooping or sniffing attacks. (Papaioannou et al. 2020) It is difficult to detect this attack because it does not create any abnormalities in the network. Security vulnerabilities in camera-attached gadgets can raise unwanted surveillance in home environments.(Solangi et al. 2018; Papaioannou et al. 2020; Pundir et al. 2020) Another such passive attack is a traffic analysis attack; the attacker can learn from the data being transferred in the network. If the information is encoded, then the knowledge is indirectly available for the user; the attack aims to understand the communication between the parties. Another such attack is a man-in-the-middle attack, like eavesdropping, but here the intruder can interfere with the connection and compromise the data being transferred. The compromise can be made by modifying, deleting, or updating the message. (Papaioannou et al. 2020; Pundir et al. 2020) Traffic monitoring attacks take place on IMDs(Somasundaram and Thirugnanam 2020)
- Deception of Data

The data collected by the IoT sensors is sent to the data warehouses using broadcasting via the Internet. This broadcast characteristic is exploited, and the data being transmitted is tampered. This tampering of data can cause life-threatening risks for patients in critical conditions. Even after the data reaches the data warehouses, the data can still tamper. Tampering of data at the data warehouse level can change the medical history of the patient. (Sun, Lo, and Lo 2019) IoT medical devices work in a trustless environment; they are subjected to multiple attacks, as stated earlier, which target the device's integrity and the data collected. Spoofing attacks are the main ways of tampering with the network as well as the data. The attacker fakes the sending address to enter the network. Piggybacking and mimicking are ways to execute such attacks. (Ahmed and Mousa 2016; Papaioannou et al. 2020) A way to tamper with the transmission data is to perform a data collision attack. Here collision is performed on purpose by instigating a sensor node to transmit the data at the same time when another node is doing it; this leads to data collision, due to which the header of the data gets changed, when this data reaches the receiving end, the receiver rejects the data after checking the header. This causes the loss of medical data. A selective forwarding attack is tampering with the data being sent to the server via a sensor. The attacker forwards some data flowing in the network and drops the rest; the damage to the data is severe when tampering is done near the base station. (Ahmed and Mousa 2016)

- Unavailability of Data
  The data collected by medical IoT devices need to be available for relevant users in a time of need. Denial of Service Attacks (DoS) makes this data inaccessible for medical professionals in such critical times. This might cause a threat to the life of acute patients. In case of myocardial infarction or a heart attack, the data collected by the sensors raises the alarm for the medical professionals to know about the condition. Still, if a DoS attack occurs, the alert won't be raised, and if the person attending the patient isn't alert enough, then the patient's life is in acute danger. (Sun, Lo, and Lo 2019) As we have seen, the data need to be available for the legitimate user without any disruption. Another way of rendering the data to be unavailable to the user is by battery drainage attack. The attacker exploits the resource constraints of the device, hence draining down the battery of the device. (Papaioannou et al. 2020) Battery drainage attacks take place on IMDs. (Somasundaram and Thirugnanam 2020) A way to make the data unavailable for the legitimate user is by keeping the network busy for a long time. A way to do so is by a desynchronization attack. The attacker tampers with the message sent by a sensor node and generates many copies with a forged sequence number. This leads the WBAN to an infinite cycle; the sensor keeps sending the same message repeatedly, which leads to wastage of resources and keeps the network jammed (Ahmed and Mousa 2016). The network can also be delayed by repeating the same message or waiting for a message to be sent. A replay attack does this. (Pundir et al. 2020)

1.2.1.2 Sensor Level

There are many security and privacy issues at the sensor level in a 3-tier IoT device used for healthcare systems. It has been seen that manufacturers at times overlook the security aspects of the device and focus on its functionality. Also, the sensors need to be compact, lightweight, and have fewer communication overheads, due to which existing security mechanisms may not be practical for medical IoT devices. (Sun, Lo, and Lo 2019) Security attacks at the device level are as follows:

- Tampering with Hardware
  IoT devices, especially sensor parts, are small and can be physically stolen, exposing the attacker's security information. A stollen device can also be reprogrammed and redeployed by the attacker to listen to the conversations without being noticed. The device could also collect data and then use it to make another attack (Sun, Lo, and Lo 2019; Pundir et al. 2020). The hardware can be tampered with by device capturing, reverse engineering attacks, tampering, side-channel attacks, and invasive hardware attacks. (Papaioannou et al. 2020) Another way of

tampering with sensor nodes is by jamming a node's action. The attacker launches a radio signal frequency of Broad Area Network (BAN), the sensor nodes that come in the range of this signal cannot send or receive data. (Ahmed and Mousa 2016)

- Localization Problems
  IoT devices are localized in a network. In this network of IoT devices, due to the design of IoT devices used in the medical sector, they can move in and out of the network coverage. Thus, it is a challenge to check these devices' movement and identify whether there is an attempt to intrude the network done by the attacker. (Sun, Lo, and Lo 2019). There are applications in which the exact location of IoT devices in the human body needs to be detected with sufficient precision and accuracy. The tampering of location information can impede the usability of the devices. (Saeedi et al. 2014)
- Self – Healing
  Self-healing allows devices to continue to render their function correctly even after a compromise. The device needs to detect the attack and deploy the appropriate action to tackle the invasion. These self-healing methods deployed cannot be bulky and oversized. The methods need to be lightweight in terms of computational complexity and network overheads. (Sun, Lo, and Lo 2019)
- Over the air programming
  Over-the-air programming is the most popular way of updating IoT devices with many sensor nodes. This process can lead to various security concerns. While updating the system, if an intruder sensor node is present in the network, it can listen to the updates and introduce foreign identities. (Sun, Lo, and Lo 2019) Most of the time, installing updates happens remotely and is not often managed by a security practioner. Over-the-air updates can lead to the introduction of malware that can compromise the device's functionality. (Kim et al. 2018)
- Forward and Backward Compatibility
  Forward compatibility is the characteristic due to which the future messages can't be read by a sensor when it leaves the network. Whereas backward compatibility is the characteristic of the sensor when it just enters the network, the past messages are not read by the sensor. Continuous communication is the key for IoT networks used for healthcare; thus, it can cause serious health-related issues for critical patients if messages aren't read. (Sun, Lo, and Lo 2019)

1.2.1.3 Server Level

The digitized medical records of patients are often stored in servers referred to as Electronic Medical Records (EMR). The security attacks targeting the servers storing EMR records can compromise the integrity of the data. (Sun, Lo, and Lo 2019) Some of the potential areas of attacks targeting servers are as follows:

- Malicious Device
  When infected with malware, the data stored in servers can negatively impact the clinical diagnosis the patient is undergoing. This malicious data can tamper with the trends being observed in the patient's vitals or can even change its treatment. (Sun, Lo, and Lo 2019)
- Intruder User
  Data stored in the personal server needs to be accessed when the patient is in a critical condition. The access of this data needs to be in the right hands. If an intruder gets access to this data, they may alter the available information, leading to life-threatening conditions for the patient. (Sun, Lo, and Lo 2019) Masquerading attacks are examples of such a threat. In this attack, an illegitimate entity poses an authorized entity to gain more privileges than authorized. The attacker may exploit the acquired permissions to perform malicious activities. An impersonation attack is another such attack. The intruder acts like a legitimate entity in an authentication protocol to access the network's resources. In simple words, the attacker gets to know one or more sensor nodes; it then updates its messages accordingly and sends the message

on behalf of that node. (Papaioannou et al. 2020; Pundir et al. 2020) In a Sybil attack, the attacker intruder node represents multiple identities in the network. This creates a problem for a geographical routing protocol, where the location information needs to be interchanged between their neighbours and the nodes. It is challenging to identify Sybil attacks due to their high mobility and unpredictable nature. The hello flood attack tries to change the destination address of the sensors' messages; this is done by fooling the sensors with high-powered radio transmission. (Ahmed and Mousa 2016) Intrusion attacks are carried out on wearable devices. (Somasundaram and Thirugnanam 2020)

- Malware Attacks
  The attacker can install malicious software in medical IoT devices, which can violate the system's security. This software is then disguised and inserted into an application to destroy data, run intrusive or destructive programs, or compromise the reliability, privacy, or accuracy of the system's data, entire operating system, or a particular application. Some commonly used malware are viruses, worms, trojan horses, rootkits, or other software-based malicious entities that can infect a system. (Papaioannou et al. 2020) A wormhole attack is made to damage the network topology. The transferred packet is copied and replayed at another location or within the same network without changing the content. This creates a tunnel between the two attackers, which will be used for data transmission; such attacks are silent add severely dangerous. (Ahmed and Mousa 2016) Table 1.1 summarizes the different types of malware and the attacks performed by them.

Malware Type	Attacks Performed on
Spyware	Authenticity, confidentiality, and integrity of the available resources
Keylogger	Authenticity, confidentiality, and integrity of the available resources
Trojan Horse	Availability and confidentiality of system resources
Virus	Availability and integrity of system resources
Worm	Available data or other such network resources
Ransomware	Available system resources
Rootkit	Availability, confidentiality, authenticity, or integrity of system resources or available data

Table 1.1. Types of Malware and its attacks (Wazid et al. 2019)

- DoS Attacks
  The attackers can send a high-energy signal to prevent the wireless network from working correctly, like the jamming attacks in the physical layer. (Sun, Lo, and Lo 2019) Another way to achieve this is by flooding the resource constraints with many requests and thereby congesting the bandwidth. (Papaioannou et al. 2020) The additional load on the base station can result in a DoS attack; this is done by initiating signaling attacks on a serving base station by activating more than required state signals for blocking it. (Ahmed and Mousa 2016)

- DDoS Attacks
  DDoS or Distributed Denial of Service attack is performed with the same motive as a DoS attack: to hamper execution. However, multiple compromised devices target the medical IoT device causing a denial of service, causing the system to crash. (Chacko and Hayajneh 2018) Another such way is by denying the resources to the authorized user; this is called resource hacking. (Anand and Routray 2017)

Table 1.2 summarizes the various layers of a network model along with the attacks that are targeted at those layers. Table 1.2 also summarizes how to counter these attacks, the type of the attack, whether it is active or passive, and the location of the attacker, whether the attack is internal, external or both.

Layer	Attack	Type of Attack	Counter Measures	Location of Attacker
Physical	Sybil Attack	Active	Direct Validation	Internal

	Jamming	Active	Channel Hopping	Internal
	Interception	Active	Jamming	Internal
	Physical Tampering	Active	Regular Monitoring	Internal
	Eavesdropping	Passive	Jamming	Internal
	Impersonation	Active	Encrypted communication	Internal
	Battery Drainage Attack	Active	Blacklisting Nodes	Internal
Data Link	Sybil Attack	Active	Direct Validation	Internal
	Collision Attack	Active	Use of hashing techniques	Internal
	Replay Attack	Active	Using timestamps on all messages	Internal
	Traffic Analysis	Passive	Encrypt traffic	Internal
	Spoofing	Active	Packet filtering	Internal
Network	Selective Forwarding Attack	Active	Multi-hop acknowledgement	Internal
	Sybil Attack	Active	Direct Validation	Internal
	Hello Flood Attack	Active	Using signal strength for comparison	Internal
	Spoofing Attack	Active	Packet filtering	Internal
	Wormhole Attack	Active	Use of cryptography and GPS	External
	Denial of Service Attack	Active	Protecting endpoints	Both
	Distributed Denial of Service	Active	Network monitoring	Both
	Masquerading Attack	Active	Code Signing	Internal
Transport	Flooding Attack	Active	Configuring firewall	Internal
	Desynchronization Attack	Active	Double authentication	Internal
	Denial of Service Attack	Active	Protecting endpoints	Both
	Distributed Denial of Service	Active	Network monitoring	Both
	Man-in-the-middle Attack	Active	Use of VPNs	Internal
Application	Spoofing	Active	Traffic filtering	Internal
	Resource	Active	Limit broadcasting	Internal

Table 1.2. Classification of attacks-based on the layer they attack

1.2.2 Privacy Issues in Medical IoT

The growing availability of IoT devices and medical applications based on data analytics captures, stores, and analyses large amounts of private patient data. Along with the security issues faced by medical IoT devices, the growing privacy issues posed by IoT applications in the medical field are equally problematic. Some of the critical problems posed are risks to confidential patient data, leakage of corporate medical data, ownership, accountability of the data, and patient location leakage. In the following section, we have given a comprehensive analysis of the various privacy issues of Medical IoT.

- User Data and Identity

  Medical IoT devices and related facilities collect real-time patient data using various body embedded and wearable devices. The enormous data generated by connected devices ensures faster and economic health care, better patient experience, and efficient workflow for healthcare professionals. However, the end-users should be concerned with how the data is handled and

stored before getting their private data exposed. Many user data is collected by medical service providers, like the type of device, contexts, frequency of measurements, measurement readings of vitals and body parameters, and history of usage (Alagar et al. 2018). This can lead to a fully interconnected web of health information onto which advanced mining and statistical analysis can be applied to leverage valuable insights.

- Data or Record Linkage
  Medical records of patients are collected and analysed concerning their demographics and behaviour. This can lead to identifying a patient and their other existing diseases uniquely. Data linkage typically involves grouping observations from multiple data sources to identify the individual's data uniquely. Various sensitive information such as mental status, sexual diseases, infectious diseases, and genetic information is derived using information linkage. This can result in privacy attacks on individuals and family health information (Madaan, Ahad, and Sastry 2018). The data linkage itself is a privacy threat, and it can also lead to other privacy problems like user profiling and data localization.
- Location Information
  This relates to the privacy of the physical location of the customers. Many personal wearable devices collect the users' current location information to send guidance or trigger specific contextual supports and services (Papaioannou et al. 2020). The hackers who gain unauthorized access to the database could expose this information. The location information can give clues regarding the places frequently visited by users and the typical occupancy timing of houses and office spaces. This can later be used to launch attacks or to conduct burglary.
- Information or Query Access
  This is related to the user's information from the database or the queries that the user initiates. The user's queries can give valuable information regarding the users' health status, medicines, and treatments. Further, this information can also be combined with linked privacy attacks to extract information regarding relatives and their friends. This can reveal various habits and activities the user engages into and can be used for targeted advertising. (JA 2015)
- Data Ownership
  Even though patient data holds a trove of vital information belonging to the patient, Is the patient the sole owner of the data? Consider the case of vital signs of patient, imaging, and investigation reports being collected at diagnostic centers; these data are retained with them for later use. Further, the doctors refer to these reports and prescribe medicines and treatments. It is evident that patient data is accessed and used by intermediaries, and thus, the patients sometimes don't even get to know who all have access to the data. Legislation must be made regarding data and patient data ownership regarding the secondary usage of data. (Koh 2019)

The importance of protecting privacy in medical IoT systems is more challenging and demanding considering the data's sensitivity in the medical healthcare industry. There are risks associated with privacy when multiple features are integrated with a single medical IoT device. Data measurements can also be less accurate and error-prone, leading to users seeking unwanted treatments.

1.3 Review of Existing Solutions

Many significant works address the privacy and security issues of medical IoT. Most of the solutions have used conventional security solutions involving encryption, authentication, access-control based and blockchain-based solutions. We have reviewed the significant research works for security attacks in medical IoT devices in the following section.

1.3.1 Mechanisms for Security Attacks in Medical IoT devices

R. Somasundaram and Mythili Thirugnanam (Somasundaram and Thirugnanam 2020) reviewed and analysed various security issues for medical IoT devices and identified solutions to such problems. The security goal is to create a public infrastructure for device-level security, utilizing a mutually robust

authentication scheme and a unique identity, a trusted public key infrastructure with a unique identity, and a robust authentication scheme. This could be achieved by applying an advanced authentication mechanism, an authentication secured socket layer, and lightweight cryptography. The goal is to achieve secure monitoring by increasing device security and identifying IoT devices' bizarre behaviour for continuous monitoring. This can be achieved by monitoring spatial information, temporal information, temperature monitoring, and frequent device status updates in other devices in the network. The next level of IoT security is prevention; the motive is to prevent threats by protecting against external threats and preliminary detection of attacks; this can be achieved by monitoring incoming packets using a pocket filtering firewall. Let's consider detection in the form of vulnerability management by identifying new vulnerabilities in IoT devices, improving IoT infrastructure security, and persistent detection; to conquer this goal, we can analyse data packets and monitor unusual data being transmitted. The next goal is to respond to the attacks by accessing system vulnerability, resolving implementation plan, and preventing possible security dangers; to do this, we need to immediately update the faults of the device to other devices in the same network; after that avoiding the readings from that compromised device.

In the following section, we investigated the different solutions for security attacks in medical IoT devices.

- Authentication Based

  Pankaj Kumar and Lokesh Chouhan (Kumar and Chouhan 2021) proposed protecting the network from various attacks using SAMA (Secure Addressing and Mutual Authentication Protocol). The proposed method uses a unique identification and addressing method for authenticating medical devices uniquely identified in a wireless IoT network. SAMA also gives anonymity during the communication between the user and the medical server, with a session key. The authors claim that SAMA protects against man-in-the-middle attacks, forward and backward secrecy, replay attack, malicious smart device deployment, privileged insider attack, device compromises, masquerade attacks, message forgery attacks, and offline password guessing. Though the prosed system was tested using the AVISPA tool.

  Maria Almulhim and Noor Zaman (Almulhim and Zaman 2018) proposed a lightweight authentication system for medical IoT devices that was group-based. This projected model used elliptical curve cryptography (ECC) principles to provide energy efficiency in medical IoT devices, mutual authentication, and computations. The system creates a secure link between the sensor and the base station. The scheme would provide individual authentication to each node with a session key agreement. To save energy and cost, they use group authentication based on the distance between the base station and sensor nodes. The sensor node would collect the data and sent it to the head node, and the collected data would be forwarded to the server by the head node via the base station. The authors claim that their proposed system is secure against unknown key sharing attacks, impersonation attacks, and man-in-the-middle attacks.

- Access Control Based

  Yang Yang et al. (Yang et al. 2019) suggested a self-adaptive access control method to preserve IoT healthcare devices' privacy. After encryption, the medical readings and files are transferred to the data store, which can be transferred to other users using cross-domain transfer protocols. While using traditional access control methods, only authorized personnel can access the patient's medical records; this creates excellent problems during a medical emergency. The patient needs to be provided with first aid, but the person providing first aid is unaware of the patient's medical history; this could lead to life-threatening complications. To overcome this, the authors offer a self-adaptive access control method, which incorporates giving access to authorized personal during regular times. Still, during a medical emergency, it gives a password-based break-glass mechanism. The proposed method also provides a deduplication

mechanism that removes all the duplicate files from the datastore. The authors proved the system to be IND-CPA secure by solving the DBDH problem.

- Encryption Based

  Entao Luo et al. (Luo et al. 2018) gave a practical framework for collecting the patient's medical data and maintaining their privacy; they named the framework as Privacy Protector. They used Slepian Wolf codding-based secrete sharing mechanisms; the proposed system would secretly share the data and repair the damaged data. A distributed database is used for storing the data of the patient. So, when an authorized user asks for a patient's information, these multiple servers send the data without seeing through the content of the data. In the traditional methods of lossless operation using XOR for encryption, we need an initial vector (IV) and count pair. Attackers can easily guess the IV-counter pair and control the plain text leading to encryption and then decryption, giving access to the data. But in this proposed system, a secrete key is given to the medical practitioner and the servers, so the attacker would not guess the IV without the key. Even if one of the many servers remains uncompromised, the patient's data will remain protected. The authors claim that they have tested their model against various attacks

  Rafik Hamza et al. (Hamza et al. 2020) gave a probabilistic cryptosystem that efficiently protects patient's privacy and protects keyframe confidentiality. The system would also reduce energy consumption and the communication bandwidth. Traditional encryption algorithms for one-dimensional data and textual data cannot be used for medical data due to the digital data properties limitations. Since the data is being transferred on exposed channels, there might be privacy loss of patients. The data being transferred must be encrypted to maintain the patient's privacy. The proposed system transfers images captured from wireless capsule endoscopy procedures using a prioritization method. The images generated after the encryption show behavioral randomness, which reduces the computational cost and brings high security. The proposed mechanism also processes the collected data without any leakage and allows only authorized personnel to decrypt the data. The proposed method used a block symmetry encryption algorithm. The proposed system was tested using the NIST test, sensitivity, NPCR, UACI, Histogram, Information Entropy, Correlation Coefficient, Key Space, Image quality, time, and performance. The proposed model is effective against statistical, differential, and all-out attacks to find the secrete key.

  Ayuman Ibaida, Alsharif, and Naveen Chilamkurti (Ibaida, Abuadbba, and Chilamkurti 2021) developed an encryption system using neural networks for transferring ECG data. A shallow neural network is used to remember the ECG pattern in few neurons. To consider the loss while converting to the neural network form, we encode the loss into a small footprint with the help of BWT (Burrow wheeler transform), run-length encoding, and MTF (move-to-front). For maintaining privacy in the network, only the neurons are encoded with the help of the session ID and session key, which is received from the health authority server every time the client wishes to transfer an ECG signal. The health authority server is only able to link the session ID to the patient. The health authority server would provide the doctor with the session key and session ID whenever the doctor wishes to see the reports and is authorized to do so. This proposed system reduces the size by 50%, giving a compression ratio of 6, reduces transfer time by 60%, and ensures security.

  Rihab Boussada et al. (Boussada et al. 2019) proposed a novel solution for privacy-preserving in medical IoT devices. The authors propose an Identity-based Encryption system (L-IBE) based on Elliptical Curve Discrete Logarithm (ECDL) problem, which defines public keys as user pseudonyms. This system provides authentication, data privacy, replay attack, and data integrity. A BPA or build path algorithm is used for communication, built on top of the L-IBE model. For validation and authentication, BAN logic and AVISPA tools are used. The proposed method is resistant to replay attacks, eavesdropping attacks, forging attacks, chosen messages indistinguishable, and time-correlation attacks. The proposed mechanism is tested for energy cost, storage overhead, computational cost, and data transmission overhead.

- Block-Chain Based

  Reyhane Attarian and Sattar Hashemi (Attarian and Hashemi 2021) proposed an anonymous protocol based on UDP to protect privacy and data in a mHealth transaction. The proposed system uses onion encryption, onion network, onion routing, and blockchain for transferring data. With the help of the identity disclosure process, the system can quickly identify malicious clients. Secure connections can be sent between two entities of the network without the need to transfer data. In this system, the client has a holding identity attribute (D) and other identity attributes (OD); after initial computations, the public and private keys are generated, and the data is sent to the verifier. The verifier verifies and authenticates D using the NIZKP of Goldwasser scheme and verifies the data OD; after verification, the data is signed and distributed on the blockchain. The admin or the health authority can register clients and ask them for their key using off-chain channels. Sending the data, they used an onion encrypted network that creates a chain between the client sending the data, onion nodes, and the hospital. The hospital which receives the data verifies the identity of the sending client using the NIZKP of Goldwasser scheme. The signed and committed data is then received from the blockchain. If the receiver is authorized to receive the data, it will use the key it received from the off-chain anonymous onion connection. The commitment is then opened, and the data is stored in the local database. The proposed system is effective against calumniating attacks, pollution attacks, forgery attacks, repudiation attacks, omissions attack, eavesdropping attacks, replay attacks, impersonation attacks, collision attacks, man-in-the-middle attacks, and Sybil attacks.

  Jafar A. Alzubi (Alzubi 2021) used Lamport Merkle Digital Signature (LMDS) to make a highly secure system for IoT devices, assisted by block chain. The model is authenticated using the Lamport Merkle Digital Signature Generation model by building a tree, where the leaf nodes signify the sensitive patient records hash function. A centralized healthcare controller uses Lamport Merkle Digital Signature Verification to determine the root. In this process, the hash value of the public key and the root is compared; if the values are equal, it is the key's root, and the signature used is valid. This method identifies malicious users with minimum computation time and overhead. The proposed solution also reduces the struggle involved in the generation and storage of the signatures. It also uses large hash values, making it difficult for intruders and attackers to attack the system. The experimental results proved that the Lamport Merkel Digital Signature technique reduced the computational time and computations overhead by 25% and enhanced the security by 7%. Another advantage of the proposed system is that it does not require any trusted third party to exchange data; the blockchain efficiently performs the required computations.

1.3.2 Mechanisms for Privacy Attacks in Medical IoT devices

- User Data and Identity Information

  Data privacy is essential in every field, and it assumes greater significance when dealing with users' health information. The research work done by Raaj Anand Mishra et al. (Mishra et al. 2021) proposed a blockchain-based privacy-preserving and tamper-proof architecture for storing identity information for students. This brought a scalable storage mechanism, and authors have developed a proof-of-concept using the Ethereum blockchain. This work could also be extended to patient data, thereby controlling the patients' ownership and privacy. AttriChain, proposed by authors Wei Shaho et al. (Shao et al. 2020), also used blockchain-based technology to develop a distributed identity governance. This provides unlikability and anonymity to legitimate users and, at the same time, provides accountability to the actions of the users. The traceability of malicious activity is distributed in the network rather than relying on single identity management. The identity privacy is preserved in AttriChain using the user's signature created using user-generated transaction keys and self-generated transaction keys. No one, including the blockchain owners, can derive the linkage between users and transactions

committed by the users in this scheme. The sender's privacy is maintained by making a signature using attribute credentials rather than using public keys.

Another important work that focuses on privacy-preserving identity access management schemes is ARIES by Jorge Bernal Bernabe et al. (Bernabe et al. 2020). The authors have used anonymous credential systems and identity protection leveraging the derived information from the users' personal information. The biometric data or any personal data collected from the user is not stored in clear text and is associated with anonymous identifiers. After the data is processed at the server, the biometric data is encapsulated in a biometric token signed and encrypted by the biometric service and sent to the user's device for storage. Thus, users' data are never stored at the server, enhancing the privacy of user data. As authors in (Wood 2020) described, building digital solutions with integrated identity management schemes is the need of the hour. There is a growing demand for identity as a Service (IDaS) where user credentials and identity information can maintain users' privacy.

- Location-Based Privacy

  Many research works help in addressing the location-based privacy issues based on the protocol stack. One of the significant works done in this direction is by (Gruteser and Grunwald 2005) that uses a technique to frequently dispose of the user's interface identifier at the Media Access Control Layer. The interface numbers of identifiers reveal the location information of the user. Another work that prevents location revealing is to associate two different IP addresses: static and dynamic. Also, security agents have been used to encrypt and route the messages in the network (Fasbender, Kesdogan, and Kubitz, n.d.). Another significant work done by authors in (Memon 2015) is the query privacy algorithm based on spatial cloaking. In this technique, mobile users' location is mapped into a region of k-1 users to maintain anonymity. This approach helps keep the anonymity of the users' location and makes a user's query differentiable from another user's query. It has contributed significantly to anonymizing the continuous query. The authors (Fawaz and Shin 2014) have developed an LP-Guardian solution for protecting the location privacy of android smartphone users using the concept of indistinguishability. This provides independent app protection and minimal user interaction. LP-Guardian provides location privacy in majorly three ways; the user's exact location is modified to the location coordinate of the center of the city; routes traversed by users are modified to a synthetic route, and in cases where users require a higher degree of granularity, the location information is obfuscated. A cognitive approach utilizing existing network resources to ensure location privacy is introduced (Han et al. 2018). The multi-server architecture proposed by the authors blocks the direct connection between the location-based queries and the query issuers. The accurate query issuer's location is not included in the query that is sent to the server. The user's queries are sent to the server through the user's social media friends, and the query results are also sent to the user through trusted third-party applications. Obfuscation-based techniques protect users' location privacy in research work done by C.A Ardagna et al. (Ardagna et al. 2007). The data collected from user's applications or sensors are perturbed artificially to reduce the accuracy of location information. The obfuscation techniques used by the authors are of three categories: Obfuscation by enlarging, shifting, and reducing the radius. These techniques can be done individually or used in combination depending on the preference of the users. The advantage of this scheme is that obfuscation techniques can be chosen depending on the users' preference. A quantitative measure will also be given to the location privacy generated with the help of the algorithm.

- Data Linkage Privacy

  Linkage of data records can reveal vital clues regarding the health information of the individual and their relationships. Many health organizations use record linkage to derive meaningful insights from multiple data sources for epidemiological study and drug research. The researchers in (Randall et al. 2014) have used the privacy-preserving record linkage technique,

reducing the risk of disclosing information. They have used encrypted personal identifying information and probability-based linkage and have proven satisfactory results compared with traditional unencrypted personal identifiers. The privacy-preserving linkage techniques can separate identity information from medical records. The data holders can use passphrases to encrypt the personal identifiers. The authors' proposed work provides a significant milestone in privacy-preserving linkage information using the bloom filter method for approximate string comparisons. This technique has proven effective for data linkage without revealing private information and could greatly benefit drawing insights from data analysis. Few other significant research works preserve privacy and realize the full potential of the data. One among them is the secure, anonymous information linkage gateway [SAIL] done by researchers Kerina H Jones et al. (Jones et al. 2014). The gateway provides access to anonymous data and all analytical capabilities on the data. It is also responsible for different security features, including firewalls, encrypted network connections, two-factor authentication methods, and security servers. It provides privacy-preserving the view and access of data-to-data users. Every data access request needs to be approved by the SAIL gateway after getting the signature of the data usage on the data access agreement. These techniques could be extended to be used in record linkage while maintaining data privacy. A comprehensive survey of privacy-preserving record linkage techniques is given in research work by authors Dinusha Vatsalan et al. (Vatsalan, Christen, and Verykios 2013). Some of the techniques described by the authors include Secure Hash Encoding, Secure Multi-party computation, Pseudorandom functions, Phonetic Encoding, Differential Privacy, Random values, etc.

- Data Access or Query Privacy

  Casper (Chow, Mokbel, and Aref 2009), the query processing for location services without compromising users' privacy is significant research in the direction of privacy-preserving query processing. The location anonymizer and privacy-aware query processor are the two integral components of this application. The user's location information is masked into spatial regions based on the privacy requirements. The privacy-aware query processor further processes cloaked spatial information instead of the exact location information. In Casper, the original data is not stored; however, a perturbed version of the data is stored. Also, the location information of the user issuing the query is anonymized. This framework provides a privacy-aware query processor that provides a minimal and inclusive answer. Another critical research work in this direction is done by Yubin Guo et al. (Guo et al. 2013) using data storage and query protocol based on homomorphic encryption. This preserves the privacy of both data owners and query users. The proposed solution is implemented using the Berkely database, a no SQL database, and the encryption and decryption process done by Elgamal and Paillier encryption system.

  A new privacy-preserving query scheme called XRQuery (Yekta and Lu 2018) is proposed by Nafiseh Izadi Yekta et al. for fog computing-based IoT networks. The proposed technique can preserve privacy from the end-user and service provider perspective. The authors have evaluated the performance of the XRQuery mechanism and have demonstrated that the communication overhead is O(log n) which is less than the existing protocol's efficiency of O(n). This is also proven to be more computationally efficient than PQuery against which the algorithm is compared.

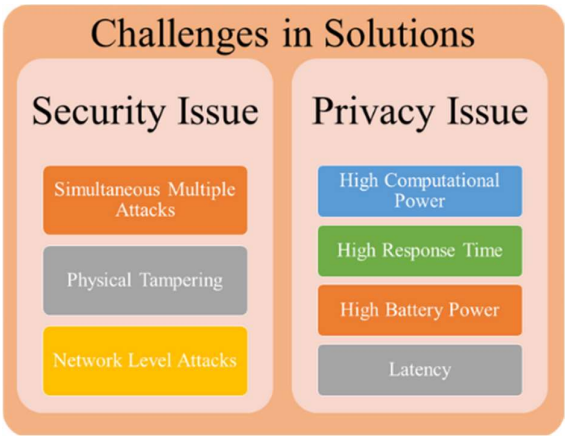
- Data Ownership Privacy

  The discussion of privacy issues of data ownership is very significant, and some of the essential works worth mentioning are described in this Section. In research work (Nawaz et al. 2020), the authors have presented EdgeBoT, a framework using edge computing that provides data ownership. This performs P2P data trade without the need for a third party through a private Ethereum blockchain. The authors have used the Elliptic Curve Cryptography technique to encrypt the data, and a child key derivation function is used to generate a unique key every

time. The authors have evaluated the performance and reliability of the model and found that the model uses only 40 % of the computing power on average. Thus, this scheme is helpful for applications to be deployed on IoT devices and medical IoT devices. Another significant work that describes the importance of blockchain-based solutions for tracking the ownership of data is done by Jong-Hyung Lee et al. (Lee and Kim 2017). They have pointed out that research in this direction can contribute to privacy and security challenges. However, they have rightly mentioned research is in nascent stages that need to be fully evolved considering the inherent security challenges.

1.4 Challenges in Existing Solutions

The intrinsic nature of medical IoT devices in terms of computational power, memory, storage capacity is often overlooked when designing security and privacy solutions. Some of the critical research gaps in this direction are summarised in Figure 1.4.



<Figure 1.4 here>

Figure 1.4. Challenges in Solutions for Security and Privacy Issues

1.4.1 Challenges in Solutions for Security Issue

Section 1.1.2.1 has discussed the solutions to various security attacks on medical IoT devices, but we need to consider all kinds of attacks and real-time scenarios. All the stated solutions were tested in a simulated system and not in real-time. In real-time, there can be multiple attacks happening at the same time. Once an attacker gets a way to enter the system, then it can send various forms of attack, are the proposed systems capable of handling all attacks at the same time with limited computational power is a matter of great concern. Physical tampering cannot be stopped as people or attackers can steal away specific sensors and may or may not replace them with tampered sensors. It is possible that the tampered sensor sends false data or be spying on the patient with spying devices fitted in the sensor node. It is vital to protect patients and the IoT network from such physical attacks.

The solution presented in (Almulhim and Zaman 2018) reduces computational costs and overheads, but group authentication raises concerns. Since the network is divided into small groups, this can attract attackers to attack such networks. Similarly, the solutions presented in (Kumar and Chouhan 2021) and (Almulhim and Zaman 2018) provide authentication security, along with security from man-in-the-middle attacks and impersonation attacks. Still, these solutions do not consider network-level attacks like denial of service, distributed denial of service, and collision attacks. These attacks prevent the use of network resources, hence rendering the system useless. In (Luo et al. 2018; Boussada et al. 2019; Ibaida, Abuadbba, and Chilamkurti 2021), the authors provide solutions for various infiltration attacks different encryption methods. This again shows the negligence of malware attacks and denial of service attacks. Homomorphic encryption schemes could be used to improve the efficiency of these cryptosystems further. (Alzubi 2021; Attarian and Hashemi 2021) Present solutions to cyber-attacks

with blockchain help, but blockchains are not entirely secure; they are also vulnerable to time jacking, transaction malleability, routing, and eclipse attacks.

1.4.2 Challenges in Solutions for Privacy Issue

In Section 1.1.2.2, we have described various solutions that exist for privacy issues for medical IoT. However, while designing the solution, we should consider the intrinsic characteristics of medical IoT devices. Medical IoT devices have constraints in battery power, memory, and processing power. Any potential solutions before being implemented should be evaluated in terms of the constraints of medical IoT devices and, very importantly, should not be a resource and computationally intensive. The privacy solutions mentioned in (Chow, Mokbel, and Aref 2009) and (Guo et al. 2013) can solve the problem of query access privacy; however, their computational power is not evaluated. At the same time, (Yekta and Lu 2018) can have lower computational requirements. The privacy solution mentioned in (Nawaz et al. 2020) has limitations in response time, thus restricting its use to static environments. This can be an impeding factor when used in dynamic medical environments when real-time data processing and analysis are required.

Data Linkage is beneficial to derive valuable insights from multiple health records and add greater value to the usefulness of the patient data. We inevitably have privacy-preserving data linkage. In research works (Randall et al. 2014) and (Jones et al. 2014), the authors have used encryption-based solutions to implement data linkage privacy; however, these research works have not evaluated how the proposed solutions impact the time taken for retrieving the data and the battery power consumed. Latency is a significant factor that should be considered. At the same time, we implement privacy-preserving solutions, and this has not been considered in most of the solutions that have been considered in our study. The techniques used to ensure identity and location-based privacy need to be evaluated for the usefulness of the information as most techniques use masking and obfuscation-based approaches.

Thus, solutions for security and privacy issues of medical IoT should be designed and implemented, focusing on the constraints of medical IoT devices and the usefulness and availability of patient data in the highly demanding dynamic environment.

1.5 Conclusion and Future Scope

We can witness an increased integration of technologies like artificial intelligence, machine learning, image mining, augmented and virtual reality combined with the Internet of things in the medical domain. Many countries have increasingly adopted innovative health care solutions mainly due to their efficiency, reachability, and cost-effectiveness. Many global health care service providers have started using IoT-based solutions for their day-to-day operations and delivery. Combining the expectation of obtaining better and quality service from smart health care and achieving lower security and privacy compromise generates extensive interest. The concerns of security and privacy of medical IoT can deter the growth of this industry that can revolutionize the medical and health care sector.

We have done a comprehensive survey of the progress of the medical IoT domain, prominent use cases, security and privacy challenges faced by smart health care applications. We have also reviewed important existing solutions for security and privacy attacks and the challenges in existing solutions. This review indicates that the way forward should be to increase the adoption of smart IoT devices in the medical field with privacy and security solutions in place suitable for resource-constrained medical IoT.

1.6 References

Ahmed, Isra'a, and Ahmad Mousa. 2016. "Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services." *International Journal of Advanced Computer Science and Applications* 7 (9). doi:10.14569/ijacsa.2016.070933.

AL-mawee, Wassnaa. 2012. "Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey," 50. https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661&context=masters_theses.

Alagar, Vangalur, Alaa Alsaig, Olga Ormandjieva, and Kaiyu Wan. 2018. "Context-Based Security and Privacy for Healthcare IoT." *Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018*, 122–28. doi:10.1109/SmartIoT.2018.00-14.

Almulhim, Maria, and Noor Zaman. 2018. "Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications." *International Conference on Advanced Communication Technology, ICACT* 2018-Febru. Global IT Research Institute (GiRI): 481–87. doi:10.23919/ICACT.2018.8323802.

Alraja, Mansour Naser, Murtaza Mohiuddin Junaid Farooque, and Basel Khashab. 2019. "The Effect of Security, Privacy, Familiarity, and Trust on Users' Attitudes Toward the Use of the IoT-Based Healthcare: The Mediation Role of Risk Perception." *IEEE Access* 7. IEEE: 111341–54. doi:10.1109/ACCESS.2019.2904006.

Alzubi, Jafar A. 2021. "Blockchain-Based Lamport Merkle Digital Signature: Authentication Tool in IoT Healthcare." *Computer Communications* 170 (January). Elsevier B.V.: 200–208. doi:10.1016/j.comcom.2021.02.002.

American Heart Association editorial staff. 2015. "Implatable Medical Devices." https://www.heart.org/en/health-topics/heart-attack/treatment-of-a-heart-attack/implantable-medical-devices.

Anand, Sharath, and Sudhir K. Routray. 2017. "Issues and Challenges in Healthcare Narrowband IoT." *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2017*, no. Icicct: 486–89. doi:10.1109/ICICCT.2017.7975247.

Ardagna, C A, M Cremonini, E Damiani, S De Capitani Vimercati, and P Samarati. 2007. "Obfuscation-Based Techniques," 47–60.

Attarian, Reyhane, and Sattar Hashemi. 2021. "An Anonymity Communication Protocol for Security and Privacy of Clients in IoT-Based Mobile Health Transactions." *Computer Networks* 190 (September 2020). Elsevier B.V.: 107976. doi:10.1016/j.comnet.2021.107976.

Bernabe, Jorge Bernal, Martin David, Rafael Torres Moreno, Javier Presa Cordero, Sébastien Bahloul, and Antonio Skarmeta. 2020. "ARIES: Evaluation of a Reliable and Privacy-Preserving European Identity Management Framework." *Future Generation Computer Systems* 102 (700085). Elsevier B.V.: 409–25. doi:10.1016/j.future.2019.08.017.

Boussada, R., Balkis Hamdane, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. 2019. "Privacy-Preserving Aware Data Transmission for IoT-Based e-Health." *Computer Networks* 162. Elsevier B.V.: 106866. doi:10.1016/j.comnet.2019.106866.

Chacko, Anil, and Thaier Hayajneh. 2018. "Security and Privacy Issues with IoT in Healthcare." *EAI Endorsed Transactions on Pervasive Health and Technology* 4 (14): 1–8. doi:10.4108/eai.13-7-2018.155079.

Chow, Chi Yin, Mohamed F. Mokbel, and Walid G. Aref. 2009. "Casper*: Query Processing for Location Services without Compromising Privacy." *ACM Transactions on Database Systems* 34 (4). doi:10.1145/1620585.1620591.

Darshan, K. R., and K. R. Anandakumar. 2016. "A Comprehensive Review on Usage of Internet of Things (IoT) in Healthcare System." *2015 International Conference on Emerging Research in Electronics, Computer Science and Technology, ICEREC 2015*. IEEE, 132–36. doi:10.1109/ERECT.2015.7499001.

Department, Statista Research. 2016. "Projected Size of the Internet of Things (IoT) in Healthcare Market Worldwide from 2016 to 2025 (in Billion U.S. Dollars)." *Medical Technology*. https://www.statista.com/statistics/997959/worldwide-internet-of-things-in-healthcare-market-size/.

Fasbender, A., D. Kesdogan, and O. Kubitz. n.d. "Variable and Scalable Security: Protection of Location Information in Mobile IP." In *Proceedings of Vehicular Technology Conference - VTC*, 2:963–67. IEEE. doi:10.1109/VETEC.1996.501454.

Fawaz, Kassem, and Kang G. Shin. 2014. "Location Privacy Protection for Smartphone Users." *Proceedings of the ACM Conference on Computer and Communications Security*, 239–50. doi:10.1145/2660267.2660270.

Gruteser, Marco, and Dirk Grunwald. 2005. "Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: A Quantitative Analysis." *Mobile Networks and Applications* 10 (3): 315–25. doi:10.1007/s11036-005-6425-1.

Guo, Yubin, Liankuan Zhang, Fengren Lin, and Ximing Li. 2013. "A Solution for Privacy-Preserving Data Manipulation and Query on NoSQL Database." *Journal of Computers (Finland)* 8 (6):

1427–32. doi:10.4304/jcp.8.6.1427-1432.
Hamza, Rafik, Zheng Yan, Khan Muhammad, Paolo Bellavista, and Faiza Titouna. 2020. “A Privacy-Preserving Cryptosystem for IoT E-Healthcare.” *Information Sciences* 527. Elsevier Inc.: 493–510. doi:10.1016/j.ins.2019.01.070.
Han, Meng, Lei Li, Ying Xie, Jinbao Wang, Zhuojun Duan, Ji Li, and Mingyuan Yan. 2018. “Cognitive Approach for Location Privacy Protection.” *IEEE Access* 6: 13466–77. doi:10.1109/ACCESS.2018.2805464.
Hoare, Daniel, Anubhav Bussooa, Steven Neale, Nosrat Mirzai, and John Mercer. 2019. “The Future of Cardiovascular Stents: Bioresorbable and Integrated Biosensor Technology.” *Advanced Science* 6 (20): 1900856. doi:10.1002/advs.201900856.
Ibaida, Ayman, Alsharif Abuadbba, and Naveen Chilamkurti. 2021. “Privacy-Preserving Compression Model for Efficient IoMT ECG Sharing.” *Computer Communications* 166 (April 2020). Elsevier B.V.: 1–8. doi:10.1016/j.comcom.2020.11.010.
JA, A. 2015. “Digital Footprints and Privacy Concerns.” *INFOSEC*. https://resources.infosecinstitute.com/topic/digital-footprints-privacy-concerns/.
Jones, Kerina H., David V. Ford, Chris Jones, Rohan Dsilva, Simon Thompson, Caroline J. Brooks, Martin L. Heaven, Daniel S. Thayer, Cynthia L. McNerney, and Ronan A. Lyons. 2014. “A Case Study of the Secure Anonymous Information Linkage (SAIL) Gateway: A Privacy-Protecting Remote Access System for Health-Related Research and Evaluation.” *Journal of Biomedical Informatics* 50. Elsevier Inc.: 196–204. doi:10.1016/j.jbi.2014.01.003.
Kim, Jun Young, Wen Hu, Hossein Shafagh, and Sanjay Jha. 2018. “SEDA: Secure over-the-Air Code Dissemination Protocol for the Internet of Things.” *IEEE Transactions on Dependable and Secure Computing* 15 (6). IEEE: 1041–54. doi:10.1109/TDSC.2016.2639503.
Kodali, Ravi Kishore, Govinda Swamy, and Boppana Lakshmi. 2016. “An Implementation of IoT for Healthcare.” *2015 IEEE Recent Advances in Intelligent Computational Systems, RAICS 2015*, no. December. IEEE: 411–16. doi:10.1109/RAICS.2015.7488451.
Koh, D. 2019. “Patient Data: Access, Privacy & Ownership.” *HealthcareITNews*. https://www.healthcareitnews.com/news/apac/patient-data-access-privacy-ownership.
Kumar, Pankaj, and Lokesh Chouhan. 2021. “A Privacy and Session Key Based Authentication Scheme for Medical IoT Networks.” *Computer Communications* 166 (October 2020). Elsevier B.V.: 154–64. doi:10.1016/j.comcom.2020.11.017.
Lee, Jong Hyouk, and Hyoungshick Kim. 2017. “Security and Privacy Challenges in the Internet of Things [Security and Privacy Matters].” *IEEE Consumer Electronics Magazine* 6 (3). IEEE: 134–36. doi:10.1109/MCE.2017.2685019.
Luo, Entao, Md Zakirul Alam Bhuiyan, Guojun Wang, Md Arafatur Rahman, Jie Wu, and Mohammed Atiquzzaman. 2018. “PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems.” *IEEE Communications Magazine* 56 (2). IEEE: 163–68. doi:10.1109/MCOM.2018.1700364.
Madaan, Nishtha, Mohd Abdul Ahad, and Sunil M. Sastry. 2018. “Data Integration in IoT Ecosystem: Information Linkage as a Privacy Threat.” *Computer Law and Security Review* 34 (1). Elsevier Ltd: 125–33. doi:10.1016/j.clsr.2017.06.007.
Memon, Imran. 2015. “Authentication User’s Privacy: An Integrating Location Privacy Protection Algorithm for Secure Moving Objects in Location Based Services.” *Wireless Personal Communications* 82 (3). Springer US: 1585–1600. doi:10.1007/s11277-015-2300-y.
Mishra, Raaj Anand, Anshuman Kalla, An Braeken, and Madhusanka Liyanage. 2021. “Privacy Protected Blockchain Based Architecture and Implementation for Sharing of Students’ Credentials.” *Information Processing and Management* 58 (3). doi:10.1016/j.ipm.2021.102512.
Mordo intelligence. 2021. “Internet of Medical Things (IOMT) Market - Growth, Trends, Covid-19 Impact, and Forcasts (2021-2026).” https://www.mordorintelligence.com/industry-reports/internet-of-medical-things-market.
Nawaz, Anum, Jorge Peña Queralta, Jixin Guan, Muhammad Awais, Tuan Nguyen Gia, Ali Kashif Bashir, Haibin Kan, and Tomi Westerlund. 2020. “Edge Computing to Secure Iot Data Ownership and Trade with the Ethereum Blockchain.” *Sensors (Switzerland)* 20 (14): 1–17. doi:10.3390/s20143965.
O’Donnell, Lindsey. 2020. “More than Half of IoT Devices Vulnerable to Severe Attacks.” *Threat Post*. https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/.
Papaioannou, Maria, Marina Karageorgou, Georgios Mantas, Victor Sucasas, Ismael Essop, Jonathan Rodriguez, and Dimitrios Lymberopoulos. 2020. “A Survey on Security Threats and

Countermeasures in Internet of Medical Things (IoMT)." *Transactions on Emerging Telecommunications Technologies*, no. May: 1–15. doi:10.1002/ett.4049.

Pundir, Sumit, Mohammad Wazid, Devesh Pratap Singh, Ashok Kumar Das, Joel J.P.C. Rodrigues, and Youngho Park. 2020. "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges." *IEEE Access* 8. IEEE: 3343–63. doi:10.1109/ACCESS.2019.2962829.

Randall, Sean M., Anna M. Ferrante, James H. Boyd, Jacqueline K. Bauer, and James B. Semmens. 2014. "Privacy-Preserving Record Linkage on Large Real World Datasets." *Journal of Biomedical Informatics* 50. Elsevier Inc.: 205–12. doi:10.1016/j.jbi.2013.12.003.

Saeedi, Ramyar, Janet Purath, Krishna Venkatasubramanian, and Hassan Ghasemzadeh. 2014. "Toward Seamless Wearable Sensing: Automatic on-Body Sensor Localization for Physical Activity Monitoring." *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC 2014*. IEEE, 5385–88. doi:10.1109/EMBC.2014.6944843.

Sarmah, Simanta Shekhar. 2020. "An Efficient IoT-Based Patient Monitoring and Heart Disease Prediction System Using Deep Learning Modified Neural Network." *IEEE Access* 8: 135784–97. doi:10.1109/ACCESS.2020.3007561.

Shao, Wei, Chunfu Jia, Yunkai Xu, Kefan Qiu, Yan Gao, and Yituo He. 2020. "AttriChain: Decentralized Traceable Anonymous Identities in Privacy-Preserving Permissioned Blockchain." *Computers and Security* 99. Elsevier Ltd: 102069. doi:10.1016/j.cose.2020.102069.

Solangi, Zulfiqar Ali, Yasir Ali Solangi, Shahmurad Chandio, Madihah Bt S.Abd Aziz, Mohd Syarqawy Bin Hamzah, and Asadullah Shah. 2018. "The Future of Data Privacy and Security Concerns in Internet of Things." *2018 IEEE International Conference on Innovative Research and Development, ICIRD 2018*, no. May. IEEE: 1–4. doi:10.1109/ICIRD.2018.8376320.

Somasundaram, R., and Mythili Thirugnanam. 2020. "Review of Security Challenges in Healthcare Internet of Things." *Wireless Networks* 0. Springer US. doi:10.1007/s11276-020-02340-0.

Spaan, Nienke A, Alina E Teplova, Eric Renard, and Jos A E Spaan. 2014. "Implantable Insulin Pumps: An Effective Option with Restricted Dissemination." *The Lancet Diabetes & Endocrinology* 2 (5): 358–60. doi:10.1016/S2213-8587(14)70035-X.

Sun, Yingnan, Frank P.W. Lo, and Benny Lo. 2019. "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey." *IEEE Access* 7. IEEE: 183339–55. doi:10.1109/ACCESS.2019.2960617.

Tarouco, Liane Margarida Rockenbach, Leandro Marcio Bertholdo, Lisandro Zambenedetti Granville, Lucas Mendes Ribeiro Arbiza, Felipe Carbone, Marcelo Marotta, and Jose Jair Cardoso de Santanna. 2012. "Internet of Things in Healthcare: Interoperatibility and Security Issues." In *2012 IEEE International Conference on Communications (ICC)*, 22:6121–25. IEEE. doi:10.1109/ICC.2012.6364830.

Vatsalan, Dinusha, Peter Christen, and Vassilios S. Verykios. 2013. "A Taxonomy of Privacy-Preserving Record Linkage Techniques." *Information Systems* 38 (6). Elsevier: 946–69. doi:10.1016/j.is.2012.11.005.

Wazid, Mohammad, Ashok Kumar Das, Joel J.P.C. Rodrigues, Sachin Shetty, and Youngho Park. 2019. "IoMT Malware Detection Approaches: Analysis and Research Challenges." *IEEE Access* 7. IEEE: 182459–76. doi:10.1109/ACCESS.2019.2960412.

Wood, Simon. 2020. "Adhering to Privacy by Design with Identity-as-a-Service." *Network Security* 2020 (7). Elsevier Ltd: 14–17. doi:10.1016/S1353-4858(20)30081-7.

Yang, Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, and Victor Chang. 2019. "Privacy-Preserving Smart IoT-Based Healthcare Big Data Storage and Self-Adaptive Access Control System." *Information Sciences* 479. Elsevier Inc.: 567–92. doi:10.1016/j.ins.2018.02.005.

Yekta, Nafiseh Izadi, and Rongxing Lu. 2018. "XRQuery : Achieving Communication-Efficient Privacy-Preserving Query for Fog-Enhanced IoT." IEEE, 1–6.

Yeole, Anjali S., and D. R. Kalbande. 2016. "Use of Internet of Things (IoT) in Healthcare: A Survey." *ACM International Conference Proceeding Series* 21-22-Marc: 71–76. doi:10.1145/2909067.2909079.