International Journal of Social Sciences Bulletin
Volume 2, Issue 4, 2024 ISSN: (E) 3007-1917 (P) 3007-1909

SECURITY AND PRIVACY CHALLENGES IN THE INTERNET OF MEDICAL THINGS (IOMT): A COMPREHENSIVE REVIEW

Shaista Ashraf Farooqi[*1], Fatima Zafar[2]

[*1]*PhD. Scholar Asia e University (AeU) Wisma Subang Jaya, Jalan SS 15/4, Subang Jaya, Malaysia*
[2]*Lecturer Computer Science Department Bahria University Karachi Campus Karachi, Pakistan*

[*1]shaista_ashraf@yahoo.com; [2]fatimazafar.bukc@bahria.edu.pk

Corresponding Author: *

Received	Revised	Accepted	Published
28 August, 2024	28 September, 2024	15 October, 2024	28 October, 2024

ABSTRACT
As technology continues to advance at a rapid pace, the Internet of Things (IoT) has emerged as a transformative force in our daily lives, with intelligent devices seamlessly integrated into our homes and workplaces, revolutionizing the way we interact with the world. However, as the IoT has expanded to include medical devices, concerns have arisen over the security of personal information and the potential for data breaches. This paper takes a closer look at the privacy and security challenges that arise with the Internet of Medical Things, exploring potential solutions to safeguard sensitive information from unauthorized access and misuse. The motivation of this review is to provide valuable insights into IoMT's context. It aims to benefit healthcare professionals, data scientists, and technologists. The study covers AI models that maintain patient privacy while enhancing patient care, nuanced techniques for data scientists, and inspiration for building secure and effective IoMT solutions for technologists. Ultimately, it seeks to empower and inform stakeholders in shaping the future of healthcare through IoMT technologies.
Keywords: *IoMT, Architecture, Security and Privacy, Federated Learning, Blockchain*.

INTRODUCTION

The Internet of Medical Things (IoMT) is a sub-branch of IoT that focuses on remote health systems. Its goal is to create a framework for real-time health monitoring and human-machine interaction, improving patient decision-making. IoMT offers cost reduction, real-time emergency interventions, and remote monitoring, but its architecture is complex due to the integration of sensory devices with the internet (Yıldırım et al.,2023) The integration of smart wearable devices has emerged as a fundamental component in the efficient processing of IoT. In the healthcare industry, the revolutionary technology of telemedicine has paved the way for remote patient monitoring, diagnosis, and disease sensing. With telemedicine, healthcare professionals can leverage smart wearable devices to remotely track patient vitals, symptoms, and health conditions, thereby enabling timely and accurate interventions. This has greatly improved patient outcomes and revolutionized the way healthcare is delivered (Nair et al., 2023). Efficient and precise diagnosis and analysis of patients' ailments is crucial in the healthcare industry. This requires continuous and thorough monitoring of extensive data. The latest healthcare systems are equipped with sophisticated technologies that offer these capabilities. However, with the emergence of intelligent healthcare systems, it has become increasingly challenging to protect sensitive patient information. As such, there is a need to develop robust and secure data protection mechanisms in the new era of intelligent healthcare (Ravikumar et al.,2023). A proficient healthcare system built upon the IoMT framework is developed in a series of stages. Initially, intelligent sensors embedded in smart wearables or implanted devices, connected through either a body sensor network

(BSN) or wireless sensor network (WSN), gather medical data from the patient's body. Subsequently, the gathered data is transmitted to a trained model via a cloud server or internet. During this phase, the patient's information is scrutinized and monitored. If any critical condition is detected, the healthcare provider will be alerted. Otherwise, the patient can proceed with their routine and follow any preventive measures as prescribed by their physician (Dhiyya et al., 2022). Implementing AI models in smart healthcare systems can remotely monitor patients with improved management experiences. These facilities provide user-end ease, especially post-COVID-19.

Managing and securing big data, especially sensitive information, poses significant challenges for researchers. This article explores vulnerabilities in IoMT architecture and outlines critical factors to consider before implementing security measures. We also discuss innovative AI model strategies that researchers use to address privacy and security concerns when handling big data.

The paper is thoughtfully structured, beginning with Section II which provides an overview of the architecture of the Internet of Medical Things (IOMT), along with an analysis of attacks on various layers. Section III then delves into the privacy and security issues that arise within the IOMT. Moving forward, Section IV offers solutions to these security concerns and attacks, while also exploring the challenges and future of IOMT. Finally, Section V thoughtfully concludes the study, while Section VI acknowledges and expresses gratitude towards those who have contributed to the paper.

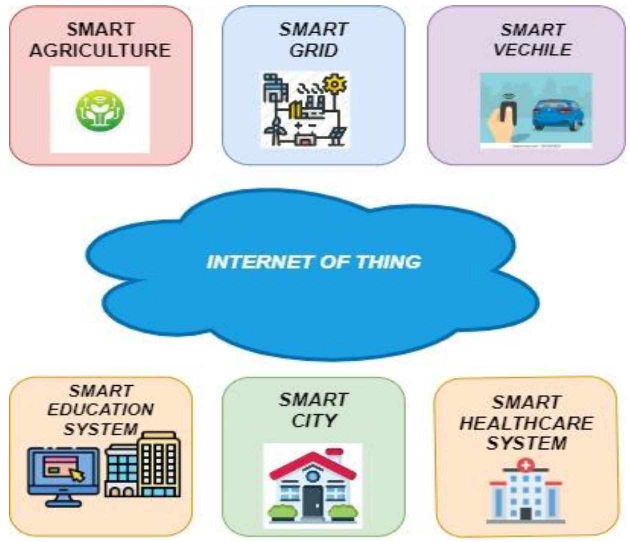

Fig. 1: Influence of IoT in everyday of life

Methodology

This research article focuses on the Internet of Things (IoT) in relation to medicine, or the Internet of Medical Things (IoMT), by considering research papers primarily published from 2018 to 2023. However, a selection of important research articles from 2016 or 2017 were also included to provide background information.

The selection process was primarily based on the reliability and reputation of the publishers, with research papers from IEEE and Springer being given priority. Additionally, a few research papers from Elsevier were also included. Out of the initial 984 papers available on IEEE, we applied exclusion criteria to filter out irrelevant ones. After further narrowing down our criteria, we ended up with a total of 887 research articles. Finally, we were able to identify 18 specific research papers that met our requirements and were worth further examination.

Our search on Springer yielded 186 research articles that were relevant to our keywords. However, we meticulously applied our exclusion criteria to narrow it down to 15 papers that we found most suitable for our analysis. From these, we carefully selected 4 papers from MDPI, 6 from Elsevier, and 4 from Wisely Online Library. This process enabled us to find the most relevant and high-quality research papers for our study.

Our research article sheds light on the importance of the Internet of Things (IoT) and how its integration with the Internet of Medical Things (IoMT) is transforming our lives. We discuss the intricate architecture of the IoT and how it is being implemented in the medical domain. Furthermore, we explore the different layers of the IoT and how each layer is susceptible to various types of attacks and threats. In our article, we not only provide a comprehensive overview of the countermeasures that can be taken to reduce the vulnerability of these attacks but also delve into advanced technical model-based solutions that can be used to mitigate these risks. Overall, our research article provides a detailed analysis of the IoT and its impact on the medical domain while also exploring the various security challenges that arise with its implementation.

Literature Review

A. IOMT Architecture

The integration of multiple layers, sensors, and device combinations into the internet creates a complex architecture for the Internet of Medical Things (IOMT). Researchers have proposed various healthcare IOMT architectures (Muhammad et al., 2019), but for the purposes of this paper, we will concentrate on discussing the primary and most uncomplicated HIOT or IOMT architecture. The Internet of Medical Things (IOMT) is structured into three layers: application, network, and perception (also known as the physical layer). Fig. 1 provides a visual representation of this fundamental structure. Designing a distinct architecture for the Internet of Things (IoT) can be challenging, as it is largely influenced by the device and its intended purpose (Pace et al., 2018). Parameters including protocol-based architecture (Sethi et al., 2017), cloud-based solutions, edge computing, and fog computing all play a role in defining the overall architecture.

2.1 PERCEPTION LAYER

The perception layer serves as a crucial conduit between healthcare institutions and smart devices. It efficiently gathers patient data and information through its two sub-layers: data access and data acquisition. The data acquisition sub-layer is responsible for procuring the data, which is then transmitted to the network layer via the data access sub-layer. To facilitate seamless communication between the layers, diverse communication technologies like Wi-Fi, Zigbee, and BLE are employed. Ensuring compatibility between specific IOMT devices and an intelligent healthcare system is crucial for their successful operation (Askar et al., 2022). The collection of data is a vital element for IOT to run effectively, and it must be done vigilantly and with great care. As the IOMT environment involves multiple entities, including smart devices, patients, and HIOT staff, it is necessary to identify and verify each entity to ensure robust IOMT performance (Khan & Alam, 2021). Unique IDs are provided to differentiate and recognize each entity. The GPRS technique is commonly used for data gathering in telemedicine and REMOTE patient monitoring (RPM) (Riđić et al., 2022), enabling interconnectivity between hardware and software. Cyber-physical system (CPS) plays a critical role in managing, controlling, and sensing the computational world and the physical world (Madhumathi & Shruthi, 2022).

2.2 NETWORK LAYER

The network layer plays a vital role in securely exchanging data from sensors or smart devices to healthcare providers. It is also responsible for collecting data from the perception layer and sending it to a specific destination within a given time frame. In this sense, the Network layer is like the backbone of the Internet of Things, acting as the brain or nervous system of the system. This layer is comprised of two sub-layers, the service sub-layer and the network transmission layer. The network layer is responsible for the IOMT architecture, based on the interoperability of multiple data and heterogeneous networks. The service sub-layer provides integration between different devices and networks, using various protocols and technologies that match the compatibility between the networks. The service support layer provides an open interface for third-party applications to develop and enhance the IOMT environment's usability (Mohammad et al., 2020).

2.3 Application layer

The highest layer of the IoMT architecture is the application layer, which serves as an interface for patients and healthcare providers. This layer includes a variety of tools, ranging from simple smartphone apps to complex computing systems for patients with severe or chronic conditions. The primary focus of the application layer is to monitor health data and manage medical information, providing medical professionals with the information they need to make informed decisions. This includes managing inpatient and outpatient records, medical equipment and facilities, and patient treatment data specific to a hospital. Additionally, the application layer includes decision-making management tools that analyze patient data and suggest appropriate treatments (Mosenia & Jha, 2016). The IoMT architecture is composed of three layers, as illustrated in Fig. 3.

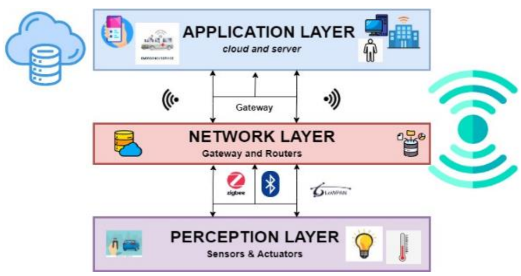

Fig. 2: Architecture of IoMT Layers

B. ATTACKS ON THREE LAYERD IoMT ARCHITECTURE

The healthcare industry has rapidly developed and embraced innovative technologies, but this has also created new opportunities for hackers to steal data. With the rise of the Internet of Medical Things (IoMT) and the Internet of Things (IoT), attackers can use similar techniques to target and compromise medical devices. It is crucial to protect our data from these new and emerging threats. IoMT systems face a wide range of threats, including spoofing, traffic analysis, masquerading, man-in-the-middle, message fabrication/modification/replay, physical, malware, denial-of-service, eavesdropping, battery drainage, and impersonation attacks (Abounassar et al., 2022).

3.1 ATTACKS IN PERCEPTION LAYER

3.1.1 SIDE CHANNEL ATTACK

There are various forms of cyber-attacks, and one of them is a channel attack that aims to extract information from a system. This information can be exploited to access a device's encryption algorithm. Side-channel attacks are a method employed to achieve this objective and can be performed through techniques like fault injection, cache attacks, and correlation attacks. Given their growing prevalence and sophistication, it is crucial to be vigilant against side-channel attacks (Makhdoom et al., 2018).

3.1.2 TAG CLONING

In this attack, the author gained access by duplicating personal credentials such as NFC (Near Field Communication) and RFID (Radio Frequency Identification) (Abosata et al., 2021).

3.1.3 PHYSICAL ATTACKS

Physical attacks are malicious techniques employed by attackers to gain unauthorized access to systems, networks, or devices by exploiting physical vulnerabilities. These attacks can be carried out through various means, such as tampering with hardware components, intercepting network traffic, or gaining unauthorized physical access to data storage devices. Some common physical attacks include stealing servers, tampering with hardware components, and using keyloggers to intercept keystrokes. It is important to implement physical security measures to safeguard against these types of attacks (Klonoff, 2017).

3.1.4 SENSOR ATTACK

Targeted cyber-attacks on IoMT sensory devices are aimed directly at the crucial components of intelligent systems that collect and transmit real-world data. Such attacks can easily compromise confidentiality, integrity, and availability (Ajagbe et al., 2022).

3.2 ATTACKS IN NETWORK LAYER

3.2.1 EAVESDROPPING ATTACKS

Insufficient security measures around the nodes can leave them vulnerable to cyber attacks. When communication between two parties is not properly encrypted, hackers can easily intercept the conversation and access sensitive information such as passwords and other personal data (Mukherjee et al., 2018).

3.2.2 DENIAL-OF-SERVICE ATTACKS

By implementing proper security measures around the nodes, we can significantly reduce the risk of cyber-attacks. Ensuring that all communication between entities is properly encrypted and secured will greatly enhance the safety and privacy of sensitive information. By taking proactive measures to strengthen security, we can safeguard personal credentials and prevent data breaches from occurring (Grassi et al., 2017).

3.2.3 MAN-IN-THE-MIDDLE ATTACKS

To ensure the safety of confidential data and information, it is important to be aware of man-in-the-middle cyber-attacks. This type of attack occurs when an attacker intercepts communication between two parties without their knowledge. Being mindful of this type of threat can help prevent a breach of valuable information (Mukherjee et al., 2018).

3.2.4 SPOOFING ATTACK:

Spoofing is a serious offense, wherein an individual gains unauthorized access to a network or system by using a false identity. This illegal activity can be executed using several methods such as IP spoofing, email spoofing, MAC spoofing, mimicking, caller ID spoofing, or piggybacking. It is essential to be aware of such fraudulent activities and take necessary measures to protect the network and system from such attacks (Franklin et al., 2020).

3.2.5 TRAFFIC ANALYSIS ATTACKS

This method of attack involves scrutinizing and observing the behavior of the target. Cybercriminals strive to comprehend the target's routine and keep tabs on their online activities without breaching their confidential data. Despite not accessing private information, this approach can still yield a plethora of details about the target, which may be exploited later. Traffic analysis can be accomplished through different techniques, including pattern recognition, meta-analysis, traffic analysis, and timing analysis (Djenna & Saïdouni, 2018).

3.2.6 MESSAGE FABRICATION REPLAY ATTACKS

Unauthorized access to IoMT devices can allow attackers to modify information by seeking passwords or other confidential information. Attackers can then alter specific data they are interested in. This method is a serious threat to the integrity and security of IoMT devices (Molina et al., 2018).

3.2.7 MASQUERADING ATTACKS

Masquerading attacks involve an individual impersonating an authorized person to gain access to restricted facilities. These attacks are particularly concerning for healthcare institutions, as they hold sensitive information pertaining to high-ranking officials. Malicious actors may attempt to access and manipulate this data to cause harm to these individuals (Makhdoom et al., 2018).

3.2.8 IMPERSONATION ATTACKS

In this attack, the attacker pretends to be an authorized user and acts as the owner. This type of cyberattack is commonly referred to as masquerading or spoofing. All three attacks work on the same principle (Lone et al., 2020).

3.3 ATTACKS IN APPLICATION LAYER

3.3.1 MALWARE ATTACKS

Malware attacks refer to the intentional use of malicious software to hack targeted systems or software, with the aim of causing harm to an organization, institute, company, or even an entire nation. Malware attacks can manifest in various forms, including Trojans, spyware, adware, botnets, ransomware, viruses, and worms. These attacks are frequently executed through phishing emails, infected software, removable media such as infected USBs and external hard drives, and malicious websites (Lone et al., 2020).

3.3.2 BATTERY DRAINAGE ATTACK

Hackers are targeting wearable devices that are used by patients, specifically those that have low-power capacity IoMT devices. The attacker typically starts by observing the power consumption range of the device and then launches a high-power usage attack. This is mainly done because these devices can gain access to the system quickly (Makhdoom et al., 2018).

3.3.3 SQL INJECTION ATTACK

SQL injection (SQLi) is an attack which provides unauthorized access, data manipulation, data leakage for entire database (Papaioannou et al., 2022).

C. PRIVACY AND SECURITY ISSUE IN IOMT

The Internet of Medical Things (IoMT) offers many benefits for patients, but it also presents significant obstacles when it comes to safeguarding the security and confidentiality of sensitive medical data. This is since medical data is comprised of personal details about patients that require exceptional care and attention. Failure to handle this data appropriately can result in severe repercussions for both patients and healthcare providers alike. As such, it is crucial to exercise extreme caution when managing medical data and to leverage intelligent IoMT technology to guarantee the protection and privacy of this important information (Molina et al., 2018).

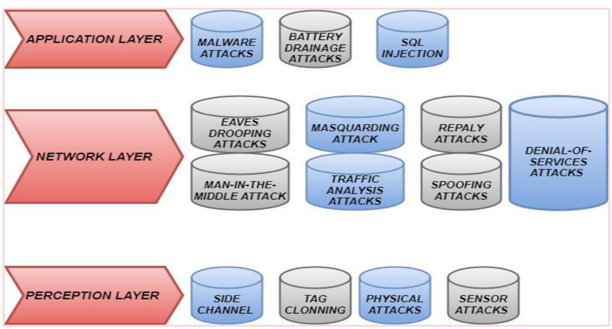

Fig 3. Attacks on Three Layer Architecture of IoMT

We focused on IoMT's security and privacy concerns and highlighted the challenges in its implementation process. It is imperative to deploy external defense mechanisms to safeguard sensitive data since smart IoMT devices lack the capability to detect attacks on their own. First, we analyze the data type and select the appropriate protection. CIANA (Confidentiality, Integrity, Availability, Non-Repudiation, and Authentication) is the basis for determining the necessary data protection measures, as explained in our survey (Klonoff, 2017).

4.1 CONFIDENTIALITY:

Effective information management is crucial in protecting confidential data from any unauthorized access. In the realm of IoMT, sensitive data is highly susceptible to malicious attacks such as eavesdropping or intrusion, making confidentiality a top priority. CIANA, a trusted authority in the field of data security, provides comprehensive guidelines and strategies for safeguarding IoMT data and ensuring its integrity and confidentiality. With CIANA's guidance, organizations can confidently navigate the complex landscape of data security and protect their valuable assets (Gupta et al., 2020).

4.2 PRIVACY

Protecting data from unauthorized access is known as data privacy. This ensures that users can utilize services without worrying about being monitored. In tele-healthcare systems, data privacy is of utmost importance. Several countries have set up agencies that monitor any suspicious online activity. The Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) are two entities that help ensure data protection. GDPR is a regulation of the European Union that safeguards the privacy of online information services (Ghubaish et al., 2020).

4.3 INTEGRITY

Ensuring data integrity is of utmost importance in safeguarding the authenticity of information. Particularly in the realm of the Internet of Medical Things, it is imperative to safeguard against unauthorized access to data. Data integrity guarantees that information remains unaltered during transmission and even when data is stored (Koutras et al., 2020). In Telemedicine, online data transmission is essential to maintain accurate patient records and treatment histories. Preserving the integrity of medical data is crucial to ensure its reliability, which is why it is strongly recommended to follow best practices for data preservation (Hatzivasilis et al., 2019).

4.4 AVAILABILITY

In the realm of telemedicine, the ability to access services around the clock is known as availability - an essential component given that patients may need medical assistance unexpectedly. As such, our IoMT system must provide constant access to medical assistance, 24/7. To maintain uninterrupted service, our system must be fortified against potential attacks, such as DOS or DDOS, which could cause it to malfunction and prevent users from accessing the service until the attack is resolved. Therefore, when designing an IoMT system, ensuring availability is our primary concern (Hatzivasilis et al., 2019).

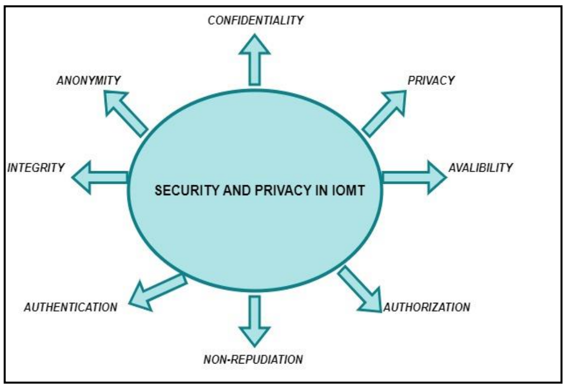

Fig4: Counter measurement for security and privacy in IoMT base devices

4.5 NON-REPUDIATION

Maintaining device integrity and authenticity is of utmost importance in any online system. To ensure lawful and regulated activity, transaction logs must be established. Responsibility is paramount when executing any actions, and once a task has been completed, it cannot be undone. Digital signatures can be added at the end of task completion to achieve non-repudiation (Yaacoub et al., 2020).

4.6 ANONYMITY

Anonymity in IoMT refers to concealing the identity of patients and healthcare providers (Lone et al., 2020). Protecting the user's end and maintaining the integrity of the system is crucial. It can help prevent passive attacks, which often occur when the attacker has knowledge of the user's activity without knowing their identity.

4.7 AUTHORIZATION

When it comes to owning property, having proper authorization is essential. In the realm of the Internet of Medical Things (IoMT), it's crucial to distinguish between legitimate and fraudulent entities to maintain a safe environment. Unauthorized access has the potential to result in disastrous consequences. Therefore, it's imperative to verify a user's identity before granting access to any service. This can be achieved through the use of a strong password or digital signature, and for added security, face scanning or fingerprint matching could be employed (Koutras et al., 2020).

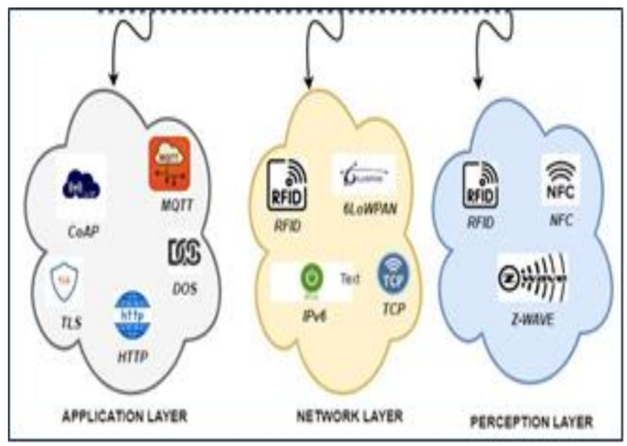

Fig 5: Communication Technologies For IoMT

D. COMMUNICATION TECHNOLOGIES FOR IOMT

The Internet of Medical Things (IoMT) is rapidly evolving, and there is a growing need for advanced communication technologies to support this growth. Communication technologies are classified into two distinct categories based on the range that they cover. Long-range communication technology supports communication across extensive network ranges, spanning several kilometers or more, whereas short-range technology is designed to operate within a smaller range of networks that are located within a few meters or less of the user. The ZigBee 6LoWPAN Network is a short-range protocol technology that has gained recognition for its reliability in the medical field. Its low latency and minimal packet loss rate make it a preferable connectivity option. One of the notable benefits of

6LoWPAN over ZigBee is its ability to communicate directly with devices. On the other hand, ZigBee offers various protocols like Wave, which can limit the number of interfaces when combining devices (Lone et al., 2020). Long Term Evolution Machine Type Communication (LTE-E), Low-Power Wide Area Networks (LoWPAN), and Low-Power Wide Area Networks (LPWAN) are advanced communication technologies that can cover large areas and transmit data up to 10 km using sub-gigahertz radio frequencies. These technologies provide long-range connectivity, even on a global scale, and offer built-in security mechanisms to support most applications. In particular, LTE-M networks provide a reliable infrastructure that can accommodate a diverse range of use cases (Yaacoub et al., 2020). The communication technology related to the three-layer IoMT architecture is illustrated in Figure 3 (Kasyoka et al., 2020).

IV. DISCUSSION

Researchers are exploring the use of Artificial Intelligence and Blockchain as leading technologies to address security and privacy challenges in the field of IoMT (Shah et al., 2020).

Blockchain Models

Blockchain technology was first introduced by Stuart Haber and W. Scott Stornetta in 1991. Since then, it has undergone many updates and improvements. In 2008, a paper titled Bitcoin was published by Satoshi Nakamoto, which introduced a peer-to-peer electronic system (Pournaghi et al., 2020). Since its inception, Bitcoin has been recognized as a powerful tool for securing IoT devices (Abdaoui et al., 2020).
MedSBA is a secure mechanism that uses a combination of CP-ABE (Ciphertext-policy Attribute-Based Encryption) and KP-ABE (Key-policy Attribute-Based Encryption) with Blockchain technology to enable secure data storage and sharing while maintaining its confidentiality (Ahram et al., 2017). Garg et al. have proposed a secure design called BAKMP-IoMT based on the Blockchain principle. This design offers a secure key management system for cloud servers, medical implantable devices, and personal servers. It has outperformed other security schemes in terms of communication, low-cost authentication, and overall security. Another Blockchain-based model is the health chain, which is a privacy-preservation strategy for large-scale health data (Xu et al., 2019).

Privacy Model

Edge computing plays a crucial role in Internet of Medical Things (IoMT) systems and is made possible by the Elliptic Curve Digital Signature Algorithm (ECDSA). This algorithm ensures data privacy during transmission from IoMT devices to the cloud. The smart devices that are used in the process are stored in the cloud, keeping them hidden, and the implementation process is simple and affordable (Deebak & Al-Turjman, 2020). In addition, reversible dual-frame data hiding is used to maintain data privacy (Gull et al., 2020). An efficient blind-batch encryption scheme based on the computational Diffie-Hellman hypothesis is also introduced for low-resource and inexpensive devices (Wang, 2019).

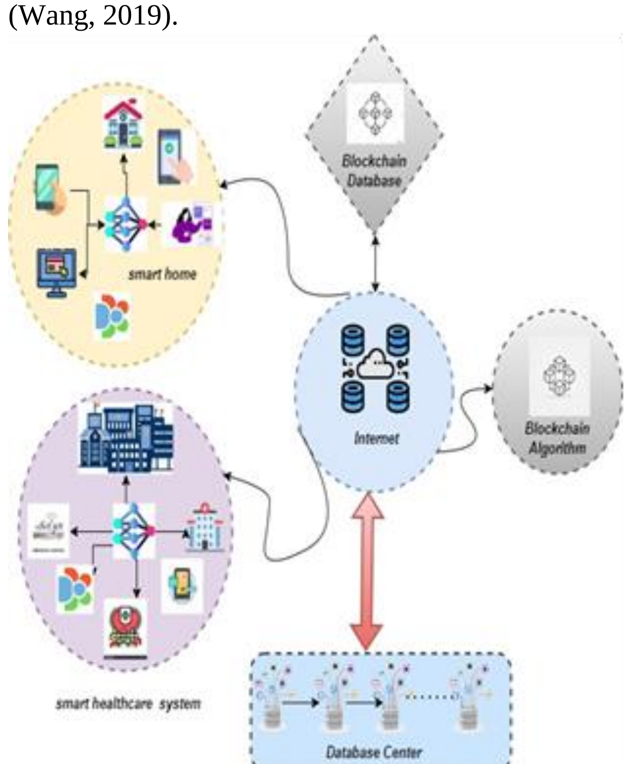

Fig 6: Basic Blockchain Model

Authentication Model

Deebak and Al-Turjman have developed a framework called Innovative Service Authentication (SSA) that verifies the user's identity. In the Network layer, the Heterogeneous Network (HetNet) uses Attribute-Based Encryption (ABE) authentication models to protect sensitive information, especially in intelligent healthcare systems. This ABE model helps reduce transmission costs and prevents unauthorized access to devices. Additionally, a secure and lightweight scheme based on Physical Unclonable Function (PUF) has been introduced to enhance the security of the IoMT device by preventing the server from storing data (Abdaoui et al., 2020).

Machine Learning Model

Based on research, it has been observed that deep learning models are capable of accurately detecting and distinguishing between genuine and fraudulent attacks. These models have a remarkable accuracy rate of 97%, making them one of the most effective tools for ensuring the safety of critical information and data within the IoMT system.

Many researchers have developed advanced deep learning models to improve security and prevent potential threats. In their research (Abdaoui et al., 2020) have created an embedded system that utilizes Raspberry Pi3 and deep learning technology to effectively classify various types of attacks. This innovative system has the added capability to differentiate between false and genuine alarms. Similarly, (Ben Amor et al., 2020) have introduced the AUDIT machine learning model, which utilizes anomaly detection and separation techniques for analyzing healthcare data from smartphones. The model's feature selection process employs correlation and PCA (Principal Component Analysis) to accurately identify authentic medical features and filter out any fabricated ones.

A team of researchers led by Priya recently published a paper outlining a machine-learning model designed to detect network attacks. Their model utilizes a combination of PCA-GWO (Principal Component Analysis-Grey Wolf Optimization) and deep learning neural network techniques for feature selection and classification, making it particularly effective for devices with a single IP address. The authors claim that their model achieves 15% higher accuracy than other existing models and reduces training and classification time by 32% (Manimurrgan et al., 2020). Furthermore, they suggest using a deep belief network for detecting intrusion attacks, as it has shown positive results in all evaluation metrics, including precision, F1 score, recall, accuracy, and detection rate.

This model is designed to operate in multiple dimensions, enabling it to detect attacks across various IoT devices and databases. It has shown an accuracy rate of 97.93% for Botnet class, 97.71% for port scan class, 97.71% for Brute force class, 96.67% for DOS/DDOS class, 99.37% for Normal class, and 96.37% for infiltration class. Additionally, it has demonstrated 98.37% accuracy in detecting web attacks (Nayak et al., 2022).

INTEGRATION OF FOG COMPUTING WITH BLOCKCHAIN

Within the realm of IoT, data gathered from sensors and smart devices is typically transmitted to the cloud layer for analysis and updates. However, this process is more intricate than it may initially appear. Directly sending data to the cloud layer requires a considerable amount of storage space and high computing power, resulting in increased costs and time consumption. To tackle this challenge, a new layer known as the Fog Layer was developed by researchers. This layer is positioned between the cloud and the user, and its nomenclature was proposed by Cisco in 2014. The term Fog signifies its proximity to the earth, and after extensive deliberation, the researchers reached a consensus on the name (Abosata et al., 2021).

Fog computing is a framework that connects different types of devices and enables seamless internet connectivity while ensuring user privacy. The primary objective of fog computing is to facilitate Device-to-Device (D2D) communication (Mukharjee et al., 2018). Figure 7 shows the increasing global demand for fog computing from 2021 to 2028.

A cutting-edge technology was introduced by Mesfer AI Duhhayyim et al. that combines fog computing and Blockchain, leveraging the YAC algorithm to verify input data. Specifically designed for health care management records within the Internet of Medical Things, the YAC (yet another consensus) protocol is utilized to power the FC-IoMT-YAC solution. Duhayyim et al. & Pavinthra et al. discuss the five critical design elements and main issues faced while developing a Blockchain-based IoT architecture. They prove that D2D architecture is better than gateway implementation. Singh and his team proposed a secure architecture for the Internet of Everything (IoE) that combines blockchain and fog computing (BFAN). The architecture ensures data security, authentication, and encryption. Nanayakkara et al. conducted a study on various attacks that could target different layers of the Internet of Things (IoT). According to their research, the most vulnerable layer to attacks and threats is the network layer, followed by the application layer. This article provides an in-depth analysis of the security and privacy concerns associated with the Internet of Medical Things (IoMT). Neshenko et al. provide a survey on IoT vulnerability and offer a preliminary look at IoT exploitation on the internet. Meanwhile, Seliem et al. present a solution to the security challenges faced by IoMT in their article titled BIoT: Blockchain for the Internet of Medical Things. The authors focus on four main key components: (i) Network cluster, (ii) cloud server, (iii) medical facility, and (iv) intelligent medical devices, each of which has a bolster. These bolsters are powerful computing devices that act as a gateway, helping to maintain security in the same way as Blockchain. In addition, Banerjee et al. discussed the position of Blockchain in the world of IoT and IoMT, emphasizing its role in securing data.

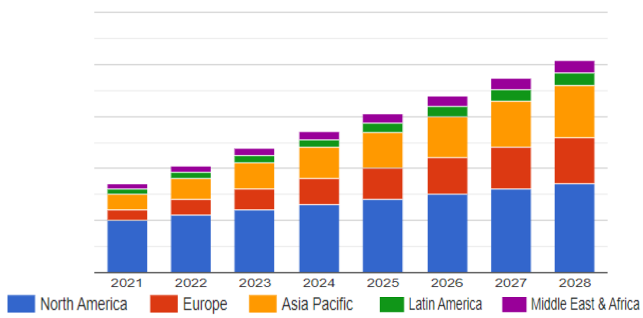

Fig 7: Show the (global market size) increase in the market of fog computing till 2028

AUTHOR	YEAR	TECHNOLOGY	DESCRIPTION
Mesfer AI Duhhayyim et al	2022	Fog computing Blockchain Yac security algorithm	Integration of Fog computing with Blockchain for healthcare data management with help of YAC algorithm security protocol
Pavithran et al.	2020	Ledger base Blockchain design	Protect the patient information from outsider or hacker
Singh et al	2020	Fog base architecture in Blockchain	A fog base architecture for the protection of data
Nanayakkara et al	2019	Privacy and security for IoMT	Security and privacy threats in IoMT especially in Network layer
Neshenko et al	2019	Cost and performance analysis in IoMT	High security for data communication in IoMT
Seliem et al	2019	Data management in IoMT	Data security of patients transmitted by the sensors
Banerjee et al	2018	Blockchain in IoMT	Data transmission between devices.

V. CONCLUSION

Our article aims to provide a comprehensive overview of the Internet of Things (IoT) in the medical field. We begin by delving into the three-layered architecture of the Internet of Medical Things (IoMT), which is the foundation of IoT in healthcare. Each layer is explored in depth, highlighting its unique challenges and opportunities.

To ensure a secure and safe environment, we identify potential threats for each layer and recommend effective solutions to prevent such attacks. Additionally, we address the concerns of privacy and security in IoT and analyze emerging technologies like Blockchain and fog computing that can help safeguard personal information.

Overall, this article offers a detailed examination of the complex landscape of IoT in healthcare, providing valuable insights for those navigating this rapidly evolving field.

References

Abdaoui, A., Al-Ali, A., Riahi, A., Mohamed, A., Du, X., & Guizani, M ((2020). Secure medical treatment with deep learning on embedded board. In Energy Efficiency of Medical Devices and Healthcare Applications (pp. 131-151). Academic Press.

Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors, 21(11), 3654.

Abounassar, E. M., El-Kafrawy, P., & Abd El-Latif, A. A. (2022). Security and interoperability issues with internet of things (IoT) in healthcare industry: A survey. Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions, 159-189.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In 2017 IEEE technology & engineering management conference (TEMSCON) (pp. 137-141). IEEE

Ajagbe, S. A., Awotunde, J. B., Adesina, A. O., Achimugu, P., & Kumar, T. A. (2022). Internet of medical things (IoMT): applications, challenges, and prospects in a data-driven technology. Intelligent Healthcare: Infrastructure, Algorithms and Management, 299-319.

Arshad, N., Baber, M. U., & Ullah, A. (2024). Assessing the Transformative Influence of ChatGPT on Research Practices among Scholars in Pakistan. Mesopotamian Journal of Big Data, 2024, 1-10.

Askar, N. A., Habbal, A., Mohammed, A. H., Sajat, M. S., Yusupov, Z., & Kodirov, D. (2022). Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT). J. Commun, 17(11), 900-918.

Baber, M., Islam, K., Ullah, A., & Ullah, W. (2024). Libraries in the Age of Intelligent Information: AI-Driven Solutions . International Journal of Applied and Scientific Research, 2(1), 153–176. https://doi.org/10.59890/ijasr.v2i1.1295

Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149-160.

Ben Amor, L., Lahyani, I., & Jmaiel, M. (2020). AUDIT: anomalous data detection and Isolation approach for mobile healThcare systems. Expert Systems, 37(1), e12390.

Deebak, B. D., & Al-Turjman, F. (2020). Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE Journal on Selected Areas in Communications, 39(2), 346-360.

Dhiyya, A. J. A. (2022). Architecture of IoMT in healthcare. The Internet of Medical Things (IoMT) Healthcare Transformation, 161-172.

Djenna, A., & Saïdouni, D. E. (2018, October). Cyber attacks classification in IoT-based-healthcare infrastructure. In 2018 2nd Cyber Security in Networking Conference (CSNet) (pp. 1-4). IEEE

Duhayyim, M. A., Al-Wesabi, F. N., Marzouk, R., Abdalla Musa, A. I., Negm, N., Hilal, A. M., ... & Rizwanullah, M. (2022). Integration of Fog Computing for Health Record Management Using Blockchain Technology. Computers, Materials & Continua, 71(2).

Franklin, J. M., Howell, G., Ledgerwood, S., & Griffith, J. L. (2020). Security analysis of first responder mobile and wearable devices. US Department of Commerce, National Institute of Standards and Technology.

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2020). Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet of Things Journal, 8(11), 8707-8718.

Grassi PA, Garcia ME, Fenton JL. NIST 800-63-3: digital identity guidelines. NIST Special Publ. 2017;68. https://doi.org/10.6028/NIST.SP.800-63-3

Gull, S., Parah, S. A., & Muhammad, K. (2020). Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare. Computer Communications, 163, 134-149.

Gupta, S., Venugopal, V., Mahajan, V., Gaur, S., Barnwal, M., & Mahajan, H. (2020, January). HIPAA, GDPR and Best Practice Guidelines for preserving data security and privacy-What Radiologists should know. European Congress of Radiology-ECR 2020.

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019, May). Review of security and privacy for the Internet of Medical Things (IoMT). In 2019 15th international conference on distributed computing in sensor systems (DCOSS) (pp. 457-464). IEEE.

Kasyoka, P., Kimwele, M., & Mbandu Angolo, S. (2020). Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. Journal of medical engineering & technology, 44(1), 12-1

Khan, S., & Alam, M. (2021). Wearable internet of things for personalized healthcare: Study of trends and latent research. Health informatics: a computational perspective in healthcare, 43-60.

Klonoff, D. C. (2017). Fog computing and edge computing architectures for processing data from diabetes devices connected to the medical internet of things. Journal of diabetes science and technology, 11(4), 647-652.

Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. Sensors, 20(17), 4828.

Lone, T. A., Rashid, A., Gupta, S., Gupta, S. K., Rao, D. S., Najim, M., ... & Singhal, A. (2020). Securing communication by attribute-based authentication in HetNet used for medical applications. Eurasip Journal on Wireless Communications and Networking, 2020, 1-21.

Madhumathi, R., Arumuganathan, T., & Shruthi, R. (2022). Internet of things in precision agriculture: A survey on sensing mechanisms, potential applications, and challenges. Intelligent Sustainable Systems: Proceedings of ICISS 2021, 539-553.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE communications surveys & tutorials, 21(2), 1636-1675.

Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access, 8, 77396-77404.

Mohammed, A. H., Khaleefah, R. M., & Abdulateef, I. A. (2020, June). A review software defined networking for internet of things. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-8). IEEE.

Mohanty, S., Mohanty, S., Pattnaik, P. K., Vaidya, A., & Hol, A. (2022). Smart healthcare analytics using internet of things: An overview. Smart Healthcare Analytics: State of the Art, 1-11.

Molina Zarca, A., Bernal Bernabe, J., Farris, I., Khettab, Y., Taleb, T., & Skarmeta, A. (2018). Enhancing IoT security through network softwarization and virtual security appliances. International Journal of Network Management, 28(5), e2038.

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602.

Muhammad, G., Alhamid, M. F., & Long, X. (2019). Computing and processing on the edge: Smart pathology detection for connected healthcare. IEEE Network, 33(6), 44-49.

Mukherjee, M., Shu, L., & Wang, D. (2018). Survey of fog computing: Fundamental, network applications, and research challenges. IEEE Communications Surveys & Tutorials, 20(3), 1826-1857.

Nair, A. K., Sahoo, J., & Raj, E. D. (2023). Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. Computer Standards & Interfaces, 86, 103720.

Nanayakkara, N., Halgamuge, M., & Syed, A. (2019). Security and privacy of internet of medical things (IoMT) based healthcare applications: A review. In 2019 IIER 750th International Conference on Advances in Business Management and Information Technology (ICABMIT) (pp. 1-18). Institute for Technology and Research.

Nayak, D. K., Mishra, P., Das, P., Jamader, A. R., & Acharya, B. (2022). Application of Deep Learning in Biomedical Informatics and Healthcare. Smart Healthcare Analytics: State of the Art, 113-132.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733.

Pace, P., Aloi, G., Gravina, R., Caliciuri, G., Fortino, G., & Liotta, A. (2018). An edge-based architecture to support efficient applications for healthcare industry 4.0. IEEE Transactions on Industrial Informatics, 15(1), 481-489.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2022). A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies, 33(6), e4049.

Pavithran, D., Shaalan, K., Al-Karaki, J. N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. Cluster Computing, 23(3), 2089-2103.

Pournaghi, S. M., Bayat, M., & Farjami, Y. (2020). MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing, 11, 4613-4641

Ravikumar, G., Venkatachalam, K., AlZain, M. A., Masud, M., & Abouhawwash, M. (2023). Neural cryptography with fog computing network for health monitoring using IoMT. Computer Systems Science and Engineering, 44(1), 945-959.

Riđić, O., Jukić, T., Riđić, G., Ganić, M., Bušatlić, S., & Karamehić, J. (2022). The Smart City, smart contract, smart health care, Internet of Things (IoT), opportunities, and challenges. Blockchain Technologies for Sustainability, 135-149.

Seliem, M., & Elgazzar, K. (2019, June). BIoMT: Blockchain for the internet of medical things. In 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (pp. 1-4). IEEE.

Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of electrical and computer engineering, 2017.

Shah, Y., & Sengupta, S. (2020, October). A survey on Classification of Cyber-attacks on IoT and IIoT devices. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0406-0413). IEEE.

Singh, P., Nayyar, A., Kaur, A., & Ghosh, U. (2020). Blockchain and fog based architecture for internet of everything in smart cities. Future Internet, 12(4), 61.

Srivastava, J., Routray, S., Ahmad, S., & Waris, M. M. (2022). Internet of Medical Things (IoMT)-based smart healthcare system: Trends and progress. Computational Intelligence and Neuroscience, 2022.

Ullah, A. et al. (2024). Analyzing the students' attitudes and behavior towards traditional classes and technology-enhanced online learning, International Journal of Social Science Archives (IJSSA). Available at: https://ijssa.com/index.php/ijssa/article/view/498

Usman, M., Asif, M., Ullah, A., & Ullah, W. (2024). User's Habits and Attitudes towards Chinese Books Reading in Pakistan. Inverge Journal of Social Sciences, 3(2), 11-28.

Wang, Z. (2019). Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected health. IEEE Internet of Things Journal, 6(6), 9555-9562.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal, 6(5), 8770-8781.

Yaacoub, J. P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 105, 581-606

Yıldırım, E., Cicioğlu, M., & Çalhan, A. (2023). Fog-cloud architecture-driven Internet of Medical Things framework for healthcare monitoring. Medical & Biological Engineering & Computing, 61(5), 1133-1147.