Jordan Medical Journal, Supplement 1, 2024
DOI: https://doi.org/10.35516/jmj.v58i2.2527

Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence

Indu Bala[1]✉, Irfan Ahmed Pindoo[2], Maad M. Mijwil[3], Mostafa Abotaleb[4], Wang Yundong[5]

Abstract

Background and Aims: The healthcare system's complex structure presents unique challenges in ensuring security and privacy. This review aimed to explore these challenges in the context of the growing integration of artificial intelligence (AI) in healthcare operations.

Materials and Methods: We conducted an in-depth analysis of the healthcare system's architecture, emphasizing the necessity of understanding its multifaceted nature to effectively safeguard sensitive data. We then assessed potential risks and vulnerabilities by reviewing previous cyber-attacks targeting healthcare institutions, establishing a basis for proposing robust countermeasures.

Results: The results highlighted the critical importance of protecting healthcare data and details the nature of threats faced by the system. Through examining past incidents, we identified common vulnerabilities and the methods by which they were exploited. Based on these insights, we propose novel strategies aimed at mitigating the impact of these security breaches in the context of healthcare.

Conclusions: The integration of AI in healthcare poses both opportunities and challenges for security and privacy. This review addressed the obstacles faced by researchers in ensuring that AI applications in healthcare are secure and respect patient privacy. We emphasized the need for continuous adaptation and improvement to keep pace with evolving threats. Ensuring the security and privacy of healthcare systems in the AI era is essential. This review identified the complexities involved to ensure security and privacy of healthcare systems and outlined proactive strategies to enhance the resilience of healthcare institutions against cyber threats. Continuous research is essential to stay ahead of potential security challenges.

Keywords: Healthcare system, Cyberattacks, Security and Privacy, Challenges.

(J Med J 2024; Supplement 1: 250–270)

Received	*Accepted*
March 31, 2024	*June 8, 2024*

INTRODUCTION

The healthcare sector's technological developments possess the capability to extend, save, and improve human lives. The technologies span a broad range, including systems that store electronic health records (EHRs), devices that monitor health and dispense medication (such as versatile gadgets, wearables, and technology embedded in the human body), and telemedicine technologies that offer remote healthcare services [1-5]. The interconnectivity of healthcare equipment is continuously progressing in tandem with their development. However, the interconnectedness of systems creates new and unique cybersecurity vulnerabilities. Cybersecurity involves protecting computer networks and their data from illegal access and intentional or unintentional disruption [6, 7].

There is increasing worry about the inadequate level of cybersecurity in the healthcare industry, which has led to compromised confidentiality of medical information and compromised integrity of data. Media reports on data breaches offer compelling proof of the exploitation of weaknesses in cybersecurity. Currently, the healthcare sector is

[1] SEEE, Lovely Professional University, Punjab, India
[2] RDC, Lovely Professional University, Punjab, India
[3] Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Iraq
[4] Department of System Programming, South Ural State University, Russia
[5] Institute of Media, Social Sciences and Humanities, South Ural State University, Chelyabinsk, Russia
✉Corresponding author: i.rana80@gmail.com

observing a significant level of emphasis and scrutiny [8, 9]. The results emphasize a substantial increase in both assaults and occurrences of medical identity theft, with attacks occurring as a result of hacking, malware infiltration, and insider threats [10, 11]. Hacking is the act of illicitly infiltrating a computer system to acquire information or create disruption. Malware, often known as "malicious software," includes programs specifically created to penetrate systems without the user's knowledge, such as viruses and ransomware [12-14].

Insider threats stem from the mistakes or intentional actions of employees, such as succumbing to phishing emails (a form of social engineering attack that seeks to acquire login credentials or initiate a malware attack), improper security configurations, password mismanagement, misplaced laptops, and transmission of unencrypted emails [15].

Conversely, external risks arise from the malevolent conduct of persons from outside the organization. Enterprise information technology (IT) security is facing a storm due to the rapid growth of data that needs to be managed, stored, analyzed, and shared, as well as the increasing complexity of cybercriminals' methods on a global level. In the beginning months of 2020, well-known companies such as Travelex and Dixons Carphone encountered publicly publicized occurrences of data breaches [16-18]. This underscores a prevalent vulnerability that the healthcare industry is not immune to.

Historically, there was a prevailing belief that healthcare systems would not be targeted for attacks, therefore leading to the perception that preventive measures were unneeded. No healthcare entity offers cybersecurity services. Traditionally, and with valid justification, the emphasis has been placed on providing medical attention to patients. Several factors contribute to the increasing vulnerability of healthcare cybersecurity as follows. (1) The utilization of interconnected technologies is becoming more prevalent to enhance the effectiveness of patient treatment, especially for individuals with chronic illnesses. This provides multiple connecting choices for medical devices. Devices are often readily available, increasing the likelihood of them being detected by a potential attacker. By circumventing the firewalls, a solitary device could provide a potential entry point to bigger hospital networks. Moreover, there is usually a time lag between the onset of an attack and the detection of the security breach, so amplifying the susceptibility to potential harm.

(2) Placing a higher priority on preserving the well-being of patients will lead to increased and continuous monitoring of patients beyond the confines of the clinical setting. The growing popularity of medical devices heightens the vulnerability to data breaches.

(3) The increasing prevalence of mobile consumer electronics, such as cell phones, has made it more challenging to safeguard health data from the risks associated with multipurpose gadgets.

(4) Numerous healthcare organizations continue to employ outdated systems in various sectors, such as Windows XP, which has not received updates since 2014. This creates a vulnerability that enables hackers and malware to evade detection effortlessly, as demonstrated by the recent WannaCry attack. Although organizations are investing in connectivity, they are neglecting to allocate sufficient funds to ensure the security and regular updating of their software and systems. This issue is worsened by a scarcity of expertise in cybersecurity within the industry due to an overall shortage of technology and the excessively high expense of cybersecurity personnel.

Consequently, the health industry is at risk of being targeted because of the swift implementation of EHR and interconnected devices, coupled with insufficient investment in cybersecurity and a failure to understand the security measures taken by healthcare professionals [19, 20]. Motivated by the points stated above, the main objectives of this review are highlighted as follows. (1) To present the detailed architecture of a typical healthcare system at the component level. (2) To explore various security and privacy issues for healthcare systems with proposal of potential combative solutions. (3) To review the existing cyberattacks in the healthcare sector and proposed solutions to combat these attacks. (4) To highlight the research community's challenges in ensuring security and privacy in healthcare systems. (5) To show the importance of AI in protecting medical data, protecting privacy, and monitoring patients. (6) Ultimately, we aimed to discuss several open challenges and future research directions for addressing security and privacy issues in health systems.

WHY THE HEALTHCARE SYSTEM IS PRONE TO CYBERATTACKS?

The healthcare sector is considered more prone to cyberattacks for several reasons as highlighted in (**Figure 1**).

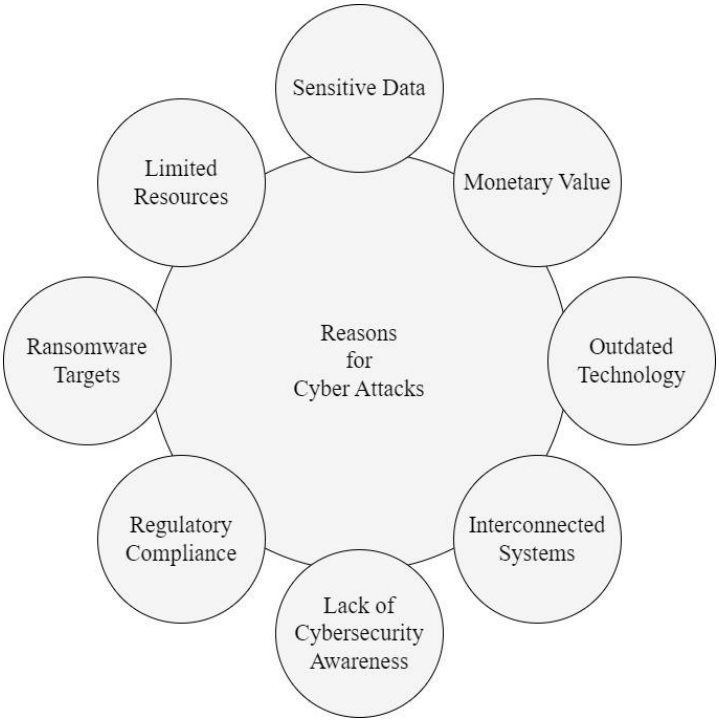

Figure 1. Reasons for Cyber Attacks

1. Sensitive Data: Healthcare firms possess an extensive quantity of sensitive and important data, encompassing patient records, medical histories, and financial information. Consequently, these individuals become appealing targets for cybercriminals who aim to pilfer personal data for identity theft, financial deception, or other nefarious endeavors.

2. Monetary Value: Healthcare data that has been stolen can be highly profitable when sold on the illegal market. Personal health information (PHI) is typically more valuable than other forms of personal data due to its potential for facilitating insurance fraud, prescription drug fraud, and even blackmail.

3. Outdated Technology: Certain healthcare systems continue to depend on antiquated technology and legacy systems that may lack adequate security protections. The rapid incorporation of emerging technology and the utilization of EHRs have occasionally surpassed the establishment of sufficient cybersecurity protocols.

4. Interconnected Systems: The healthcare industry is experiencing increased interconnectivity through the utilization of electronic health records, health information exchanges, and other digital platforms. Although this connectedness improves communication and medical care, it also expands the vulnerability of cybercriminals to launch attacks.

5. Lack of Cybersecurity Awareness: Healthcare personnel may lack the same level of vigilance and expertise in cybersecurity as experts in other industries. Occasionally, the emphasis on providing quality care to patients supersedes the importance of promoting and educating about cybersecurity.

6. Regulatory Compliance: Healthcare firms are required to adhere to stringent rules, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Adhering to these compliance standards might pose difficulties, and certain firms may give precedence to compliance rather than taking proactive cybersecurity measures.

7. Ransomware Targets: Ransomware attacks, characterized by cybercriminals encrypting data and demanding payment for its release, have shown a growing prevalence within the healthcare sector. Healthcare businesses are more inclined to pay ransoms promptly to swiftly regain access to essential systems due to the crucial importance of patient care.

8. Limited Resources: Several healthcare businesses, particularly those of smaller scale, may possess restricted resources for cybersecurity. This can render them susceptible to assaults, as they may lack the resources to invest in cutting-edge security

systems or employ expert cybersecurity personnel.

To tackle these difficulties, healthcare organizations must give priority to cybersecurity, allocate resources to acquire advanced and secure technology, consistently upgrade their systems, provide training to employees, and engage in collaboration with cybersecurity specialists to enhance their defenses against cyber threats.

A SMART HEALTHCARE SYSTEM ARCHITECTURE

A healthcare system typically comprises one or more medical devices equipped with diverse sensors to gather patients' vital signs and do independent assessments to provide advanced therapies [21-23]. The overall structure of a healthcare system is illustrated in (**Figure 2**). We delineate five crucial elements that are often required for the overall functionality of a healthcare system. The five components consist of a medical device, a sensor, networking capabilities, data processing capabilities, and a healthcare provider.

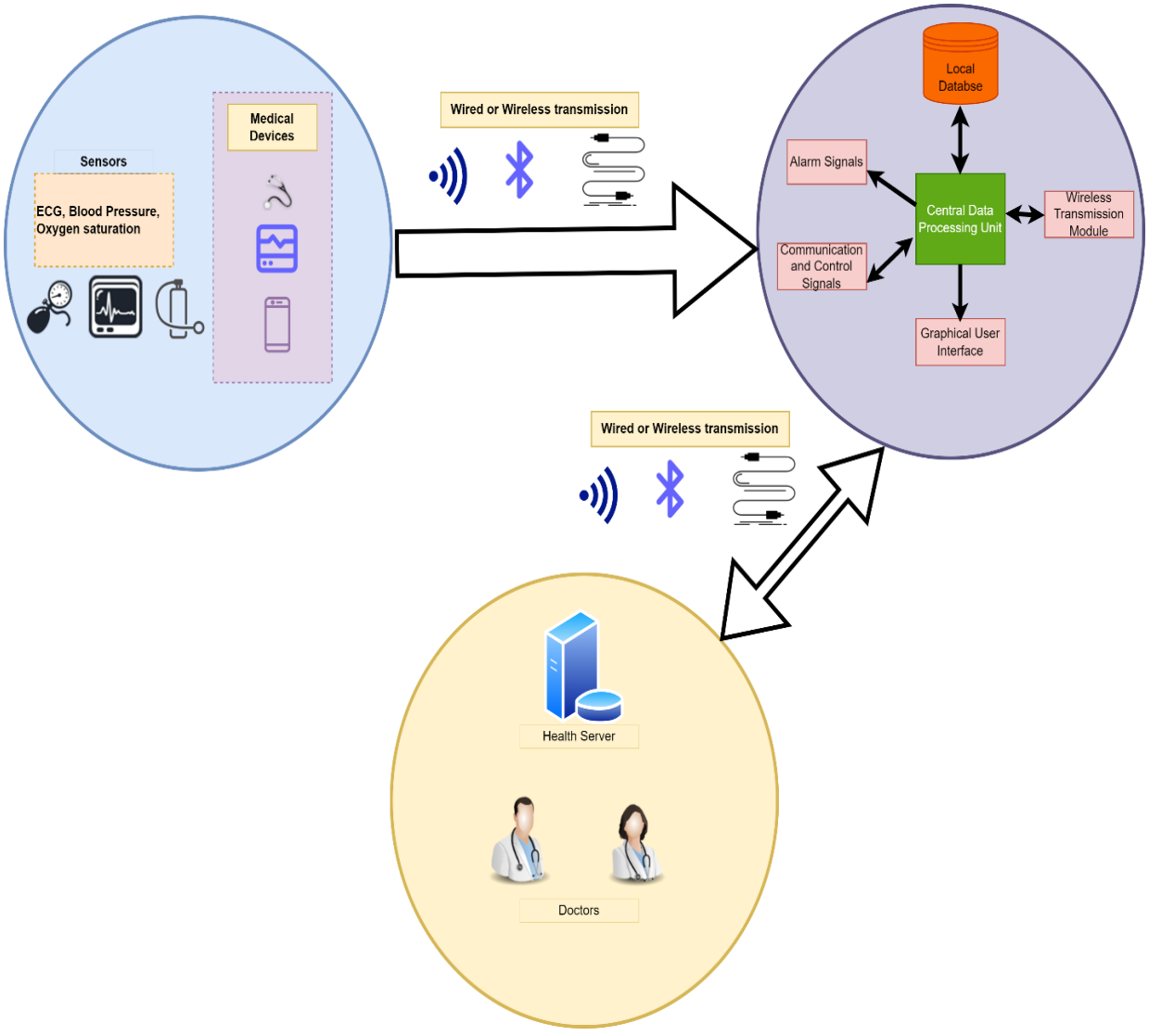

Figure 2. Smart Healthcare System Architecture

1. Medical Device: A medical device refers to any equipment, instrument, appliance, or gadget designed for one or more medical purposes, including diagnosis, monitoring, treatment, and alleviation [24]. According to the Food and Drug Administration (FDA), medical devices encompass a wide spectrum, ranging from simple tongue depressors to intricate programmable implantable cardioverter-defibrillators (ICDs) [25, 26]. The FDA categorizes medical devices according to their capacity to inflict harm on patients in the case of device malfunction or deliberate attacks. Class I medical devices, such as elastic bandages and dental floss, are considered to have a low risk and are subject to a minimal level of regulatory supervision. Class II devices, characterized by their increased complexity and higher level of danger compared to Class I equipment, require strict regulatory controls. Examples of Class II devices include pregnancy testing kits and motorized wheelchairs. Implantable pacemakers and breast implants are classified as Class III devices due to their elevated risk and intricate nature, necessitating stringent regulatory supervision. Furthermore, the European Commission establishes certain supplementary categorization criteria for medical devices, which are categorized according to their non-invasive, invasive, and active therapeutic characteristics [27].

2. Sensors: In the healthcare industry, sensors are employed to monitor and quantify a patient's vital signs [28]. Physiological sensors, such as blood sugar sensors and heart rate sensors [29, 30], act as catalysts for automating many processes inside healthcare systems, including diagnostics and monitoring. Sensors can be categorized into three distinct groups as follows: (1) Physiological sensors: These sensors measure physiological data (e.g., electrocardiogram (ECG), electromyography) and characteristics to provide a real-time estimate of the patient's health status. (2) Biological sensors: These sensors gather data on biological components in the human body, such as alcohol and glucose. They work with a physical and chemical transducer to generate electrical signals that help complete the data collection process [26, 31]. (3) Environmental sensors: These devices can detect a variety of environmental characteristics to detect any change in the patient's surroundings. These devices can be used to measure the accelerometer and gyroscope in the smartwatch and generate patterns to study patient movement and sleep data.

3. Networking: Networking components facilitate connectivity between various medical devices, sensors, and other system components. This system consists of two main stages: In the first stage, the physiological signal is sent through sensors to the central node of the system. In the second stage, the collected measurements are sent from the central node to the health center or health care workers for review. Wired or wireless technologies can be used to achieve short-range data transmission. Nevertheless, the use of wired communication may impede a patient's mobility and comfort. Autonomous sensor nodes can create a Body Area Network (BAN) by using a primary star topology network to transport data to the central node of the BAN.

IEEE 802.15.1 (Bluetooth) and 802.15.4 (Zigbee) are commonly used wireless communication technologies in Wireless Personal Area Networks (WPANs), specifically in Body Area Networks (BANs) [32]. These technologies are part of the 802.15 working group. Bluetooth is a widely accepted standard for establishing short-range connections between portable and fixed devices using radiofrequency (RF) technology. The standard runs in the unlicensed 2.4-GHz spectrum and is characterized by its low power consumption and affordable cost. The device utilizes frequency hopping technology (FHSS) across 79 channels in the industrial, scientific, and medical (ISM) bands to avoid interference [33]. It can achieve speeds of up to 3 Mbps in the enhanced data rate mode and has a maximum transmission range of 100 meters. The Zigbee standard also strives for cost-effective, low-data-rate, and durable battery solutions. The system operates on sixteen channels within the 2.4-GHz ISM band, with a data rate of 250 kbps and Offset quadrature phase-shift keying (OQPSK) modulation. Additionally, it utilizes ten channels within the 915-MHz band, with a data rate of 40 kbps and Binary Phase-shift keying (BPSK) modulation [26]. Lastly, it employs one channel within the 868-MHz band, with a data rate of 20 kbps and BPSK mode. Additional ways of communication within a BAN include infrared data association (IrDA), ultra-wideband (UWB), and medical implant communication service (MICS). UWB is an inexpensive protocol designed for the transmission of data utilizing infrared light over limited distances [34]. MICS is a wireless communication service designed for transmitting small amounts of data to support the operations of medical devices used for diagnosis or treatment. It operates on low power and does not require a license. The device functions inside the 402-405 MHz frequency range, utilizing 300 kHz channels. Various wireless technologies such as BPSK, Global

System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), Worldwide Interoperability for Microwave Access (WiMAX), and Long Range (LoRa) can be used for long-distance communication between a healthcare system and a health server or healthcare provider. These technologies offer wide network coverage and universal access. Furthermore, forthcoming developments in 5G mobile communication networks are expected to provide global Internet accessibility at significantly higher data speeds, facilitating the acquisition of real-time data from distant medical devices. The implementation of Z-Wave and Bluetooth Low Energy (BLE) is expected to lead to increased adoption of these energy-efficient communication protocols by a wider range of devices.

4. Data Processing: At this stage, the data obtained from the sensors is processed, analyzed, and features are extracted from them. The quality of this unit is essential because it connects to medical devices and borrowing devices and contains a database to store all patient data. In addition, through this unit it is possible to obtain important data about patients and monitor their health condition through data processing.

5. Health Provider: The healthcare provider component consists of health servers and medical professionals. They establish communication with the data processing component using a wireless transmission module. The healthcare server securely saves data on a remote cloud-based storage system. Healthcare professionals have access to this data to provide remote or in-person treatment to patients.

SECURITY AND PRIVACY ISSUES IN MODERN HEALTHCARE SYSTEMS

To ensure an acceptable level of privacy, the healthcare system must adhere to multiple overarching security and privacy criteria. The surveys have revealed more than twenty security needs, as detailed by the authors. As a result of limited space, we simply highlight the most essential criteria.

1. Access Control: Access control refers to the ability to restrict and manage the access of authorized users to resources. The system incorporates three separate security and privacy prerequisites: authentication, authorization, and identification. Identification, although not inherently a security risk, plays a crucial role in user authentication. Therefore, it is employed to modify the verification process of users. Authentication ensures that the user who is seeking data access is genuine, valid, and possesses the necessary identity claims before being granted access. Furthermore, it confirms the authenticity of the communication with an authorized individual. Finally, the authorization process determines, according to the security policy, whether sections of data might be restricted from external requesters. A crucial aspect is to implement an access control mechanism that safeguards patient confidentiality while also ensuring a balance between availability and confidentiality, as stated by security objectives.

2. Availability: Availability refers to the characteristics of a system and resource being easily unrestricted, functional, and ready for use by approved users at any given time and in any place throughout the healthcare system. It must be ensured that the equipment does not malfunction or experience power outages, and the systems must be continuously updated to provide safe electronic medical services to patients.

3. Dependability: Dependability assures a seamless recovery of medical information at any time, regardless of network dynamics or the occurrence of loss nodes. In most medical matters, a lack of accurate data from network issues threatens the patient's life and causes severe damage. Therefore, dependability also encompasses the system's capacity to handle and recover from errors effectively, ensuring that trust is maintained through consistent and reliable access to crucial medical data.

4. Flexibility: Flexibility in a healthcare system refers to the system's ability to adapt its rules about who can access certain medical data in emergency situations. If a patient is in critical condition and the usual rules about who can see their information are too strict, it could delay treatment and endanger their life. Therefore, flexibility ensures that in emergencies, healthcare providers can quickly get the information they need to help the patient, even if those providers are not typically authorized to access that data.

TYPES OF CYBERSECURITY ATTACKS

Cybersecurity attacks in the healthcare system can have serious consequences, including compromised patient data, disruption of medical services, and potential harm to patients [35, 36]. As illustrated in (**Figure 3**), various types of cyber threats pose risks to healthcare organizations. Some common types of cyber security attacks in the healthcare system include:

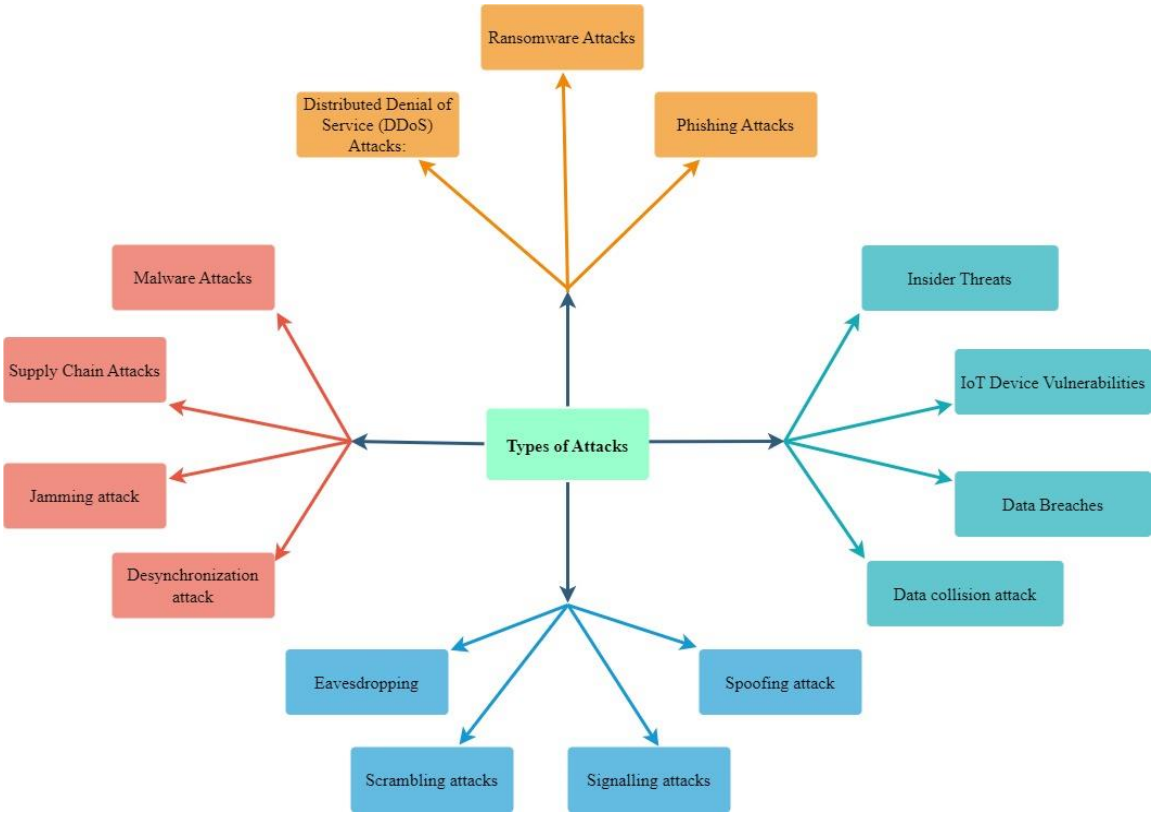

Figure 3. Classification of Cyber security attacks in the healthcare industry.

1. Ransomware Attacks: Ransomware is a type of malware that encrypts a victim's files or systems, rendering them inaccessible. Attackers then demand a ransom payment in exchange for decrypting the data. Ransomware attacks can disrupt healthcare services, making patient records and critical systems unavailable. This can lead to delays in patient care and potentially compromise patient safety [37].

2. Phishing Attacks: Phishing involves tricking individuals into providing sensitive information, such as usernames and passwords, by posing as a trustworthy entity. If healthcare staff fall victim to phishing attacks, attackers may gain unauthorized access to patient records or other sensitive information [38].

3. Distributed Denial of Service (DDoS) Attacks: DDoS attacks overwhelm a system, network, or website with a flood of traffic, rendering it inaccessible to legitimate users. DDoS attacks can disrupt online healthcare services and prevent access to critical medical information, affecting patient care [39].

4. Insider Threats: Insider threats involve individuals within the healthcare organization who misuse their access privileges for malicious purposes or unintentionally compromise security. Insiders may intentionally leak sensitive information, compromise patient privacy, or inadvertently introduce malware into the system [40].

5. Malware Attacks: Malware, including viruses, worms, and trojan horses, can infect healthcare systems and compromise their functionality. Malware can lead to the unauthorized access, theft, or destruction of patient data. It can also disrupt healthcare operations [41].

6. IoT Device Vulnerabilities: Internet of Things (IoT) devices in healthcare, such as medical devices and wearables, may have vulnerabilities that attackers can exploit. Compromised IoT devices can lead to unauthorized access to patient data, manipulation of medical equipment, or disruption of healthcare services [42].

7. Supply Chain Attacks: Cybercriminals may target the supply chain of healthcare organizations to compromise software, hardware, or services. Supply chain attacks can introduce vulnerabilities into healthcare systems, potentially leading to data

breaches or other security incidents [43].

8. Data Breaches: Data breaches involve unauthorized access to sensitive information, such as patient records, leading to exposure or theft. Data breaches can result in the compromise of patient privacy, financial losses, and reputational damage to healthcare organizations [44].

9. Jamming attack: This directs to the interference of an attacker's radio broadcast with BAN frequencies. As long as the jamming signal persists, sensor nodes within the range of the attacker signals are isolated and prevented from sending or receiving messages with other afflicted nodes and sender nodes [45].

10. Data collision attack: It arises when multiple nodes attempt to transmit simultaneously, often associated with jamming attacks where an attacker deliberately induces collisions by sending multiple messages on the channel. When collisions occur, altering the structure header, the error-checking mechanism at the receiver detects it as an error, leading to the rejection of incoming data. Consequently, any modification to the data structure header poses a threat to data availability. In a BAN Data Flooding Attack, the attacker inundates the victim node with numerous connection requests until its resources are depleted, initiating a flooding attack [46].

11. Desynchronization attack: In this type of attack, the attacker tampers with messages between sensor nodes by copying them multiple times to one or both endpoints of the active connection using a spoofed sequence number. This pushes WBAN to an endless loop, causing sensor nodes to transmit messages and waste energy repeatedly [47].

12. Spoofing attack: In this sort of attack, the attacker targets the routing information to do many disruptions, such as spoofing, modifying, or replaying the routing information, hence causing the network to become more complicated by establishing routing loops [48].

13. Sybil attacks: The malevolent attacker node embodies multiple personas within the network, posing substantial challenges for spatial routing protocols. These protocols rely on the exchange of location data among nodes and their neighboring nodes to efficiently route packets with geographic addresses. However, Sybil attackers, with their erratic behavior and rapid movement, present a formidable challenge in terms of identification [49].

14. Eavesdropping: The surveillance system is designed to gather health data from BANs and transmit it to healthcare providers. However, with wireless technology, unethical engineers could easily craft devices to intercept patient data. Therefore, when creating a system to safeguard patient information from eavesdropping and reduce the risk of theft or privacy breaches, developers must assert strict control and authority [50].

15. Data tampering attack: where a tampering attacker may damage and replace encrypted data by authorized network nodes [51].

16. Scrambling attacks: These are a type of radio frequency jamming attack designed to disrupt the regular operation of a WiMAX network during the transmission of control or management information frames. They disrupt communication, preventing the patient's smartphone from transmitting data [52].

17. Signaling attacks: Prior to transmitting data from the patient's smartphone, several preliminary signaling tasks must be carried out with the primary base station. These tasks involve authentication, key management, registration, and establishing an IP-based connection. However, an attacker can initiate a signaling attack against the base station by activating additional state signals, causing a heavy load on the base station and resulting in Denial-of-Service (DoS) attacks. Consequently, the patient's smartphone is unable to transmit data due to the unavailability of the base station [53].

To mitigate these risks, healthcare organizations should implement robust cybersecurity measures, including regular security audits, employee training, and the use of advanced security technologies. Additionally, compliance with regulations such as HIPAA is crucial to ensuring the security and privacy of patient information [54].

SECURITY SCHEMES IN MODERN HEALTHCARE SYSTEMS

Security and privacy requirements are more challenging in modern healthcare systems as compared to any other internet-based system [55-57]. Based on each level's functionalities, different security and privacy needs exist at each level of the healthcare system. This section analyzes and discusses these requirements in detail (**Figure 4**).

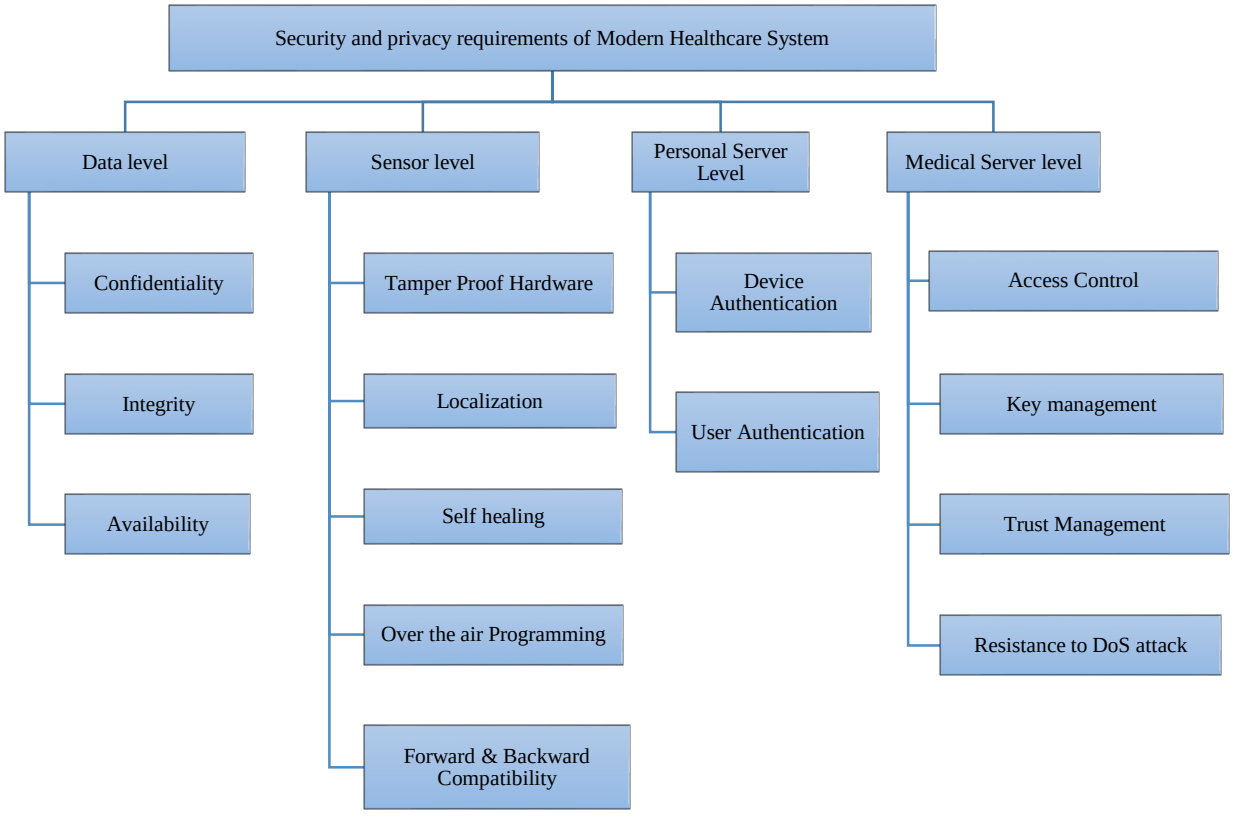

Figure 4. Security and privacy requirements for modern healthcare system.

A. Data level

1. Confidentiality: Medical confidentiality is a set of rules that restricts access to information shared between a patient and a doctor or healthcare provider [58, 59]. The patient's medical information given to health care professionals should not be divulged to others without the patient's approval. Patient health data must be collected and stored according to legal and ethical privacy rules, such as the General Data Protection Regulation (GDPR) and the HIPAA, which restrict access to authorized personnel only. Appropriate steps must be taken to preserve the confidentiality of health data associated with individual patients to prevent possible breaches. The significance of such measures cannot be overstated, as data stolen by cyber criminals could be sold on black markets not only putting patients at risk of privacy breaches but also financial and reputational repercussions. Thus, after the processing of patient personal data, if it is no longer required, it should be erased from the database permanently, except for archiving, scientific, historical, or statistical purposes.

2. Integrity: Data integrity refers to the process of ensuring the quality, efficiency, and consistency of data throughout its life cycle [60, 61]. It involves keeping patients' private information, diagnostic reports, laboratory test reports, etc. in the healthcare industry. For health practitioners and researchers, preserving data integrity is the most challenging task. Each country strives to have a computerized healthcare record of the patients to yield better services to the patients in the future with the least infrastructure requirements. However, the process of computerization of healthcare records poses serious concerns to security experts. Attacks on confidentiality, privacy violations, and information breach risk are constantly growing problems. Among all these issues, maintaining data integrity is the most critical issue. The tampering with the health records may cause a life-threatening situation to the patient. For the typical healthcare industry, the purpose of the data integrity requirement is to ensure that the data reaches the intended destination without compromise during wireless transmission. Since the attackers could gain access to the data during

wireless transmission and alter the patient data that could lead to a life-threatening situation. To ensure that the data has not been compromised, appropriate mechanisms should be incorporated to prevent data alteration by malicious attacks [62]. Moreover, the integrity of the data stored in the medical servers also needs to be ensured, which means the data cannot be tempered.

3. Availability: The digitization of the patient records is a dire need in the present scenario thus, the services and data must be accessible to the healthcare professionals whenever or wherever it is required [63, 64]. This crucial information collected from various medical servers and devices could be inaccessible in case DoS attacks occur. The situation could lead to life-threatening incidents, for example, the inability to generate quick alerts by the device in the case of a heart attack. Therefore, to accommodate the possibility of data availability loss, healthcare applications or gadgets must be always on to ensure data availability to the medical practitioners and for the emergency services. Moreover, healthcare professionals must restore the patient's data promptly to avoid DoS attacks.

B. Sensor Level

With the busy lifestyle of people, people have started adopting E-health services in which crucial health information is being collected with the help of sensors with limited power backup and computational capabilities. The security and privacy of the data collected by these sensors are always a big concern. The most common method to ensure the security of data collected from these sensors is to put this data on the personal server level. Moreover, the security measures of these sensors require a lightweight authentication protocol with less communication overhead.

1. Tamper-Proof Hardware: To collect vital health information the sensors, especially ambient sensors, can be stolen physically which could lead to information exposure to attackers. Furthermore, the stolen sensors/devices can be reprogrammed by attackers and can be redeployed to the system without being noticed to track communications. Therefore, to avoid the data tempering from these devices/ sensors, Physically Unclonable Functions (PUFs) which are security features to uniquely identify and authenticate devices based on their inherent physical variations must be used to secure data of these devices.

2. Localization: Healthcare technologies use two types of sensor localization, namely (1) on-body sensor position and (2) sensor's/patient's location [65, 66]. On-body sensor localization is important to determine whether the sensors are placed in an accurate body position. This position identification is of vital importance for applications such as activity recognition. Meanwhile, sensor/ patient localization is used to locate the patient wearing the sensor within or outside the building. Due to the mobility features, these sensors/ wearable devices could move in or out of the network's coverage range; real-time sensor detection is needed if the network authorizes its detectors to leave and rejoin irregularly.

3. Self-Healing: Self-healing features of the sensors or wearable electronic gadgets used in healthcare allow devices to resume operation after security attacks. To do so, the devices should be able to notice and analyze the type of attack, and the implementation of the appropriate security mechanisms without human intervention. Moreover, these methods must be lightweight with the least communication overheads to the network.

4. Over-the-air Programming (OTA): is widespread these days for updating devices with new patches related to security and policies [67-69]. It includes the updating or introduction to security situations such as malicious sensor node identification and forging identity details updating to the network. However, while implementing OTA, all security measures must be taken to stop the exploitation of these updates by attackers.

5. Forward and Backward Compatibility: In healthcare systems, the faulty sensors must be changed/replaced frequently with new ones. However, the sensors must have Forward and backward compatibility features. Here, the term forward compatibility means that messages transmitted by the sensors must not be readable by medical sensors once they left the network. On the contrary to this, backward compatibility means previously transmitted messages must not be readable by sensors that are just entered into the network.

C. Personal Server Level

In a typical healthcare system, the data is collected and aggregated on the personal server level before forwarding to the medical servers. Thus, it is mandatory to protect the data on the personal server level. Generally, two types of authentication strategies are used to ensure security and privacy at the personal server level, namely (1) device authentication, and (2) user authentication.

1. Device Authentication: A personal server such as a smartphone is used to store the patient data received from various sensors and medical devices. Thus, they must have some sort of authentication

before accepting data from these sensory devices. The authentication scheme must establish secured/encrypted communications to maintain data integrity and confidentiality. Alteration of patient data by malicious devices can have serious adverse effects on clinical diagnosis and care decisions; thus, device authentication should be implemented in sensor-based healthcare systems. Device authentication is mutual between personal servers and devices. Still, most of the analysis must be performed on personal servers because they often have more computational capacity and power than medical devices and sensors.

2. User Authentication: The data accumulated on the personal servers either temporarily or permanently must be accessed by the patients and medical practitioners. Accordingly, effective user authentication strategies are needed. Personal servers used for smart healthcare systems should provide patient data access in emergencies such as a stroke or a seizure. To do so, biometric authentication of the personal server level can be used as it is easy to collect such information from the sensory devices worn by the patient in the form of medical or healthcare devices.

D. Medical Server Level

Fulfilling the security and privacy requirements of the patient information at the medical server level requires: (1) the patient's information accessed by authorized devices and medical practitioners only and (2) data encryption before storing it in the databases. Since the trend of digitizing paper-based medical records is increasing rapidly, the security and privacy concerns with the medical servers are also increasing. Therefore, proper security measures must be taken into consideration at the medical server level for smart healthcare systems.

1. Access Control: Effective access control policies should be implemented to ensure that only authorized devices and personnel can access medical servers. It is difficult to ask patients for permission or consent every time they request data access, so service providers on medical servers must give patients optional access. This means they can share any data they don't have, and third parties may choose and have access. A popular alternative solution is Attribute-Based Encryption (ABE), which is classified as public-key cryptography in which a private key is derived from attributes (i.e. received signal strength, location, and channel frequency). In an ABE, accesses can be selectively designed with attributes so that only attributes that satisfy the tree are allowed access to encrypted data and treatment servers are also able to reconfigure access routes successfully. Policy updates can be unnecessary for medical servers; for instance, many cloud security systems require changing encryption keys when updating access control policies, as decryption and re-encryption of data on medical servers and individual servers is accomplished. Thus, new scalable and less redundant programming algorithms should be used to reduce or eliminate cryptography's computational cost. A famous solution is 2-layer over-encryption, where reprogramming can be done at the surface encryption layer (SEL) while data owners set additional encryption on the BEL. In addition, emergency access to patient data on medical servers can be facilitated through specific security policies. For instance, using proxy re-encryption (PRE), data encrypted with a patient's public key can be transformed into a format that a third party can decrypt in emergencies. This ensures that critical information is accessible when needed, while maintaining security under normal circumstances.

2. Key Management: Designing secure applications is based on a key management system, which seeks to use cryptographic keys and distribute them to sensor nodes. Trusted servers are critical elements of pre-distribution. Two main types of key management systems are employed in Internet of Medical Things (IoMT) healthcare systems [70-72]. Trusted server protocols get a master compromise in the network at a trusted base station. These types of protocols are suitable for hierarchical networks, but even then, reliable server protocols cannot provide vital applications such as healthcare because a comprehensive network failure can cause a reliable server to be paralyzed in real-time. Key pre-distribution protocols are commonly used in symmetric key cryptography to distribute secret keys before the network is fully functional. Such protocols are more suitable for resource-limited sensor networks because they are straightforward to execute and do not require convoluted calculations.

3. Trust Management: Trust means a bidirectional relationship between two trusted nodes, such as a sensor node and a network coordinator, that share data. For wireless healthcare applications to be successful, there must be distributed collaboration among the network nodes. In this consideration, the extent of trust of a node may be determined with trust management structures, which can be essential, mainly because evaluating a node's conduct, including the shipping, and sharing of information, is critical in healthcare applications.

4. Resistance to DoS Attacks: **Figure 5** lists

common DoS assaults against wireless healthcare packages. Attackers can use excessive-energy signals to stop the wireless community from working well, which includes jamming assaults within the bodily layer. Many strategies have been proposed to secure networks and prepare for such attacks, such as theft protection and competition strategies, but all of them are in the early stages of research [73]. Therefore, because wireless consumption is used in mobile and for dynamic reasons, real-time IoMT healthcare -Systems need more research to develop strategies to protect systems from DoS attacks.

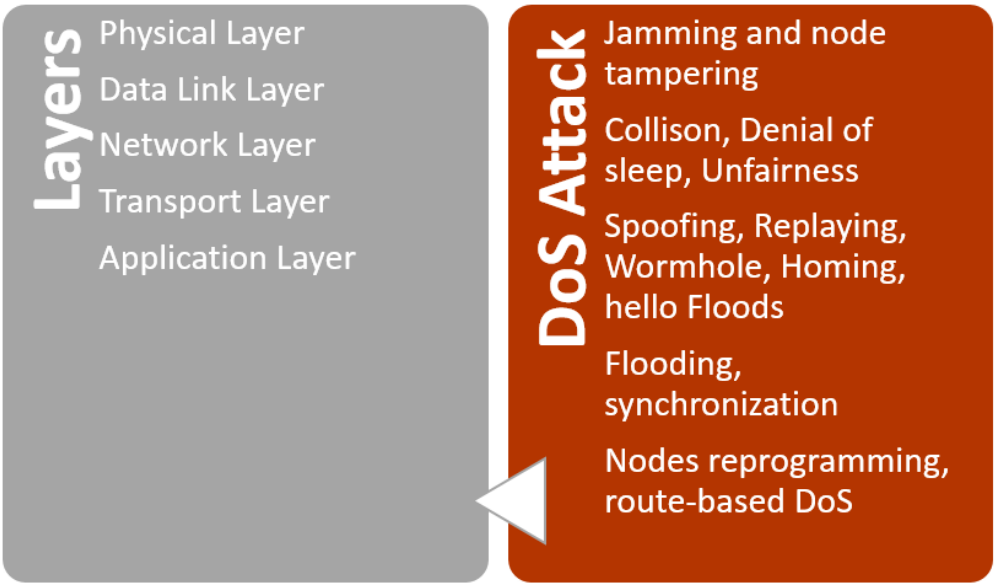

Figure 5. The most famous DoS attacks against wireless healthcare applications.

OPEN ISSUES AND CHALLENGES

A. IoMT-based Healthcare Systems

Healthcare systems based on the IoMT typically comprise three tiers: the sensor tier, personal server tier, and medical server tier. This configuration is a common feature in numerous newly proposed IoMT-based healthcare frameworks. At the sensor tier, medical devices and sensors form a local network, often referred to as a Body Sensor Network (BSN) [74]. Wireless communication at the sensor and personal server tiers often relies on low-power standards such as BLE, Near-Field Communication (NFC) [75], and radio-frequency identification (RFID) [76]. BLE is used in different network topologies in order to communicate data between parts of the network, where a connection is made between the star and mesh network. There are important technologies, namely NFC and RFID, which facilitate the provision of low energy through instant communications to the nearest device, and they can be used to monitor patients because they are implantable devices. These elements are integral to many recently proposed IoMT-based healthcare frameworks, where medical devices and sensors are deployed at the sensor layer, forming a local area network commonly referred to as a BSN.

Physiological records accumulated through clinical gadgets can be sent to personal servers, which may be on-body devices, such as smartphones, software, tablets, or off-frame devices, along with routers and gateways. The motive of personal servers is to technique and shop sufferers' information domestically earlier than sending it to the centralized clinical servers. A non-public server is needed to operate generally whilst the community connection to the clinical servers is misplaced. Medical employees, inclusive medical physicians, can get admission to patients' information remotely, supplying active recommendations to the sufferers. Applications and PC packages for early diagnoses and rehabilitation development checks can also be run on the scientific servers with patients' consent. Many IoMT-based total healthcare systems have been suggested for non-stop patient monitoring for a long time. Regardless, many of them no longer assume any safety and privacy criteria in their

designs or disregard destiny work, which includes MobiCare. This review targets other layout-demanding situations, such as power consumption and usability, instead of the security of the systems and the privacy of patients' data. Newly suggested IoMT-based healthcare systems, including BSN-Care, have followed encryption and authentication techniques in their methods.

B. Network and Protocol Design Challenges

A protocol defines a set of rules governing the exchange or transmission of data among devices. Specifically, a routing protocol dictates how network routers share data, furnishing them with necessary information to select the optimal path between any two nodes within the network or communication systems. Routing protocols in wireless networks are notably more intricate compared to those utilized in wired networks, encompassing considerations such as network topology, power conservation, and channel relevance. As a result, efficient data transfer between nodes is a multifaceted challenge in wireless network routing protocols.

1. Postural Body Movements: Physical medical devices and sensors are typically located in a group-based anatomical positioning because the patients being diagnosed or the users being monitored are rarely stationary, leading to frequent network topology and component changes. The navigation system in BSNs must adapt to frequent and unpredictable changes, such as communication links between sensor nodes, which vary as a function of time against body motion and can be involved in guidance systems to conserve energy. For instance, a transmission power control scheme based totally on the gait cycle for BSNs has been suggested, where transmission time is optimized with matching hyperlink first-rate adjustments because of taking walks. On the other hand, there are unpredictable modifications in link pleasant due to signal blockage using clothes or bags that intensify channel attenuation.

2. Temperature Rise: Two factors driving temperature increase in sensor nodes are antenna radiation absorption and power consumption of node circuitry. Radio power absorption by tissues can lead to tissue warming, signal attenuation, and potential skin or tissue burns. Consequently, routing protocols must account for transmission and computing power in sensor nodes, with particular emphasis on implant sensor nodes due to the risk of heat damage to human body tissues and organs.

3. Energy Efficiency: Routing protocols within IoMT systems must prioritize energy efficiency to optimize local energy consumption of sensor nodes and extend the overall network lifespan. Energy performance stands as a critical aspect of IoMT frameworks, influencing device size, system longevity, and usability. For example, surgical interventions may be necessary to replace batteries in implanted sensor nodes, posing risks and significant expenses. Implantable devices like pacemakers require battery lifespans of at least ten to fifteen years to sustain normal user activities. Moreover, frequent charging or battery replacements for wearable sensor nodes often impede their usability.

4. Transmission Range: Short transmission range activity can cause issues in communication disconnection and re-partitioning between sensor nodes in IoMT systems. The number of patient or user sensor nodes should be reduced to reduce disruption, providing fewer paths to nearby sensor nodes. Thus, if the connected sensor node is not far away, the packets have to be routed through a different path, resulting in higher energy consumption in that path and longer time for the packets to reach the destination. In BSNs, if the alternative path includes one or more implantable devices, the routing protocol has to be able to decide whether or not to take this alternative path primarily based on the significance of the contents within the packets.

5. Heterogeneous Environment: In numerous applications of the IoMT, a variety of sensor nodes sourced from various medical equipment providers are necessary to capture distinct physiological signals from patients or clients. Consequently, routing protocols need to be tailored to address the complexities of diverse environments found in numerous BSN setups. Several BSN platforms and frameworks have been suggested to address this issue with examples like DexterNet, which enable collaboration among different vendors to alleviate these challenges.

6. Quality of Service (QoS): BSN applications that are critical for real-time health monitoring, such as ECG sensing, are sensitive to data loss and time constraints, necessitating the fulfillment of QoS standards. However, since embedded sensor nodes have constraints in memory and processing capabilities, it's essential to implement QoS measures, such as error correction strategies for retransmissions, within routing protocols without adding a significant computational burden to the sensor nodes.

GENERATIVE AI CHALLENGES AND CYBERSECURITY CONSIDERATIONS IN HEALTHCARE SYSTEMS

The integration of generative AI into healthcare systems signifies a groundbreaking shift, heralding

advancements in patient care, diagnostic precision, and operational efficiencies that were previously unattainable [77-80].

Despite these benefits, the integration of generative AI in healthcare is accompanied by significant challenges. This includes ensuring the privacy and security of sensitive patient data, navigating the ethical and legal complexities of AI decisions, achieving seamless integration and interoperability with existing healthcare IT infrastructures, and adapting the healthcare workforce to leverage AI technologies effectively [6, 77, 80, 81].

The integration of generative AI in healthcare, while promising, introduces a spectrum range of cybersecurity challenges and ethical considerations. One primary concern is the potential for AI systems to be exploited in cyberattacks [82]. For example, if not properly secured, these systems can be manipulated to generate false data or misleading medical predictions, which could have severe negative consequences for patient care and privacy [83]. Additionally, the proliferation of AI-driven technologies increases the surface area for potential breaches, as every point in an AI system—from data input to model training and output—can be a vulnerability [84].

Another significant challenge is the issue of data bias and the reliability of AI-generated outcomes [77]. AI systems are only as good as the data they are trained on, which if flawed or biased, can lead to inaccurate medical predictions and treatments, exacerbating health disparities.

In response to these challenges, robust cybersecurity measures must be implemented. This includes employing advanced encryption for data in transit and at rest, rigorous AI system testing to detect and mitigate vulnerabilities, and continuous monitoring of AI operations to prevent and respond to potential cyber threats [85]. Additionally, fostering a culture of cybersecurity awareness among healthcare professionals and patients is vital [86].

Future trends likely will focus on enhancing generative AI's defensive capabilities, developing anomaly detection systems that can predict and neutralize threats before they impact the system, and creating transparent AI systems that allow for easy tracking and understanding of data processing and decisions [87, 88]. This is essential not only for maintaining security but also for building trust among users and regulatory bodies.

FUTURE RESEARCH DIRECTIONS

With the popularity of other emerging approaches, such as cloud computing, the IoMT security and privacy research community must fully exploit some interesting future research directions. The following are a few potential research directions in the role of IoMT security and privacy healthcare policies.

1. Blockchain: It was designed to securely store financial ledger records so that the blockchain's "blocks" are interdependent. It will also be employed with deliverable medical information stored on a medical server, delivering robust and broad security and privacy protection for IoMT health systems. Nevertheless, blockchain technology demands significant computational resources to generate blocks, which may not be feasible for IoMT devices due to their limited capabilities. On the other hand, blockchain can effectively be used to secure and store electronic health records on medical servers. A notable example of this application is MedRec, which has pioneered research into using blockchain to manage access to medical data.

2. Artificial Intelligence (AI): Machine learning and deep learning have become the most well-known analysis matters in almost every industry, including network security. In recent years, many devices gaining knowledge of total network intrusion detection strategies have been submitted, and they can also be involved in IoMT healthcare structures. As medical service providers tend to use deep learning techniques for diagnosis, the use of such techniques for systems security and privacy is also an example of research to consider, where PHI is searched at different layers of IoMT systems to detect centralized attacks through deep learning networks.

3. Security Assessment: Research teams usually conduct individual security assessments; there are no standards for assessing the security capabilities of the proposed IoMT security team. Adversarial analysis is one of the tools researchers use to determine the safety of their research. However, these adversarial analyses are based on different concepts and principles and cannot be compared. The assessment model is a web-based IoMT security assessment framework (IoMT-SAF) where recommendations can be made based on user input. Nevertheless, this work needs to consider the security strengths of existing checks or provide crypto checks for cryptographic algorithms. Further analysis is needed to assess IoMT healthcare systems' security capabilities.

The configuration of communication and protocols presents multifaceted challenges that span

various environments. Of primary concern is achieving scalability, ensuring that networks can accommodate growing numbers of devices, users, and services without sacrificing performance or security. Communication poses another vital challenge, requiring protocols to provide seamless communication across disparate systems and platforms. Security remains a perennial challenge, with the ever-evolving risk scenery disturbing strong encryption, authentication, and the right of entry to manage mechanisms to guard sensitive data and thwart malicious actors. The proliferation of rising technologies such as the IoT, edge computing, and 5G networks introduces complexities related to aid constraints, latency minimization, and fine-of-provider optimization. Moreover, the growing reliance on cloud computing and allotted architectures underscores the importance of designing resilient, fault-tolerant networks to mitigate disruptions and ensure continuous availability. Addressing those demanding situations calls for a holistic technique that integrates standards from laptop technology, engineering, arithmetic, and cybersecurity to forge progressive solutions that propel the evolution of networking paradigms toward more performance, reliability, and adaptability in the face of evolving technological landscapes.

CONCLUSIONS

This review highlighted the scope of mechanisms that should be enforced to reduce security and privacy concerns within healthcare systems to keep data from being tampered with or deleted. This review is practical in developing healthcare services by evaluating the performance of modern technologies in protecting patient data and how to benefit from them in developing the work environment and helping healthcare workers monitor patients with complete confidence. This review concludes that modern technologies have a major role in protecting data from electronic attacks by proposing innovative strategies to mitigate future threats. In addition, it focuses on improving the quality of electronic healthcare services and educating patients on how to utilize these technologies while maintaining the privacy of their data. It also addressed the role of generative AI and its applications, especially the importance of ChatGPT in developing healthcare systems. This application is considered an essential tool for developing medical research and practices within hospitals and clinics and improving healthcare quality. Thus, it is required to continuously develop this application from data and improve its performance in order to benefit from its services in obtaining more accurate results while establishing mechanisms to protect the ethical and legal nature of using this application or others in health care services and educating patients, doctors and specialists. To employ the ChatGPT application or other applications supported by AI in healthcare, all results generated from these applications must be subject to expert review to ensure their validity and possibility of application in the healthcare sector and improve patient outcomes.

This manuscript is submitted in the special issue "Evaluating Generative AI-Based Models in Healthcare"

REFERENCES

1. Aceto G, Persico V, Pescapé A. The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. Journal of Network and Computer Applications 2018;107:125-154.
2. Dang LM, Piran MJ, Han D, Min K, Moon H. A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 2019;8(7):768.
3. Salman Shukur B, Khanapi Abd Ghani M, bin Mohd Aboobaider B. Digital Physicians: Unleashing Artificial Intelligence in Transforming Healthcare and Exploring the Future of Modern Approaches. Mesopotamian Journal of Artificial Intelligence in Healthcare 2024;2024:28-34.
4. Lepore D, Frontoni E, Micozzi A, Moccia S, Romeo L, Spigarelli F. Uncovering the potential of innovation ecosystems in the healthcare sector after the COVID-19 crisis. Health Policy 2023;127:80-86.
5. Apell P, Eriksson H. Artificial intelligence (AI) healthcare technology innovations: the current state and challenges from a life science industry

perspective. Technology Analysis & Strategic Management 2023;35(2):179-193.
6. Mijwil M, Mohammad A, Ahmed Hussein A. ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. Mesopotamian Journal of CyberSecurity 2023;2023:18-21.
7. Javaid M, Haleem A, Singh RP, Suman R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications 2023;1:100016.
8. Paul M, Maglaras L, Ferrag MA, Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express 2023;9(4):571-588.
9. Merlo V, Pio G, Giusto F, Bilancia M. On the exploitation of the blockchain technology in the healthcare sector: A systematic review. Expert Syst. Appl. 2023;213(PA):18.
10. Cen M, Jiang F, Qin X, Jiang Q, Doss R. Ransomware early detection: A survey. Computer Networks 2024;239:110138.
11. Aishwarya D, Manali D. A Review of the State of Cybersecurity in the Healthcare Industry and Propose Security Controls. Mesopotamian Journal of Artificial Intelligence in Healthcare 2023;2023:82-84.
12. Vasani V, Bairwa AK, Joshi S, Pljonkin A, Kaur M, Amoon M. Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. Electronics 2023;12(20):4299.
13. Ali G, M. Mijwil M. Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles. Mesopotamian Journal of CyberSecurity 2024;4(2):20-62.
14. Gupta M, Akiri C, Aryal K, Parker E, Praharaj L. From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. arXiv 2023;2307.00691
15. Yang Y, Lin Y, Li Z, Zhao L, Yao M, Lai Y, et al. GooseBt: A programmable malware detection framework based on process, file, registry, and COM monitoring. Computer Communications 2023;204:24-32.
16. Alchi AN, Dodiya KR. Demystifying ransomware: classification, mechanism and anatomy. Perspectives on Ethical Hacking and Penetration Testing: IGI Global; 2023, p. 171-192.
17. Zhang W, Chen Z, Chen D, Li J, Pan Y. DID-IDS: A Novel Diffusion-based Imbalanced Data Intrusion Detection System; 2023, p. 364-369.
18. O'Dell E. Closing off the Warren of Negligence Claims for Data Breaches. Data and Private Law (Hart Studies in Private Law, Bloomsbury, 2023) chapter 2024;10
19. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin M-V, Calcavecchia F, Anderson D, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making 2020;20(1):146.
20. Thomasian NM, Adashi EY. Cybersecurity in the Internet of Medical Things. Health Policy and Technology 2021;10(3):100549.
21. Kalid N, Zaidan AA, Zaidan BB, Salman OH, Hashim M, Muzammil H. Based Real Time Remote Health Monitoring Systems: A Review on Patients Prioritization and Related "Big Data" Using Body Sensors information and Communication Technology. Journal of Medical Systems 2017;42(2):30.
22. Banos O, Villalonga C, Damas M, Gloesekoetter P, Pomares H, Rojas I. PhysioDroid: combining wearable health sensors and mobile devices for a ubiquitous, continuous, and personal monitoring. ScientificWorldJournal 2014;2014:490824.
23. Salman Shukur B, Mohd Yaacob N, Doheir M. Diabetes at a Glance: Assessing AI Strategies for Early Diabetes Detection and Intervention. Mesopotamian Journal of Artificial Intelligence in Healthcare 2023;2023:85-89.
24. Saini G, Budhwar V, Choudhary M. Review on

people's trust on home use medical devices during Covid-19 pandemic in India. Health Technol (Berl) 2022;12(2):527-546.

25. Stern AD. Innovation under Regulatory Uncertainty: Evidence from Medical Technology. J Public Econ 2017;145:181-200.
26. Yang M, Wang L, Lu H, Dong Q. Advances in MXene-Based Electrochemical (Bio)Sensors for Neurotransmitter Detection. Micromachines 2023;14(5):1088.
27. European Commission. MEDICAL DEVICES: Guidance Document—Classification of Medical Devices [cited 2024 26 March 2024]. Available from: https://ec.europa.eu/docsroom/documents/10337/attachments/1/translations/en/renditions/pdf.
28. Khan Y, Ostfeld AE, Lochner CM, Pierre A, Arias AC. Monitoring of Vital Signs with Flexible and Wearable Medical Devices. Adv Mater 2016;28(22):4373-4395.
29. Ding S, Schumacher M. Sensor Monitoring of Physical Activity to Improve Glucose Management in Diabetic Patients: A Review. Sensors (Basel) 2016;16(4):589.
30. Siddiqui SA, Zhang Y, Lloret J, Song H, Obradovic Z. Pain-Free Blood Glucose Monitoring Using Wearable Sensors: Recent Advancements and Future Prospects. IEEE Rev Biomed Eng 2018;11:21-35.
31. Flynn CD, Chang D, Mahmud A, Yousefi H, Das J, Riordan KT, et al. Biomolecular sensors for advanced physiological monitoring. Nat Rev Bioeng 2023:1-16.
32. Hanif M, Haque AKMF. Wireless Body Area Network: An Overview and Various Applications. Journal of Computer and Communications 2017;5:53-64.
33. Tröster G. The Agenda of Wearable Healthcare. IMIA Yearbook of Med. Informatics 2005;14
34. Mazhar F, Khan MG, Sällberg B. Precise Indoor Positioning Using UWB: A Review of Methods, Algorithms and Implementations. Wireless Personal Communications 2017;97:4467–4491.
35. Soni P, Pradhan J, Pal AK, Islam SH. Cybersecurity Attack-Resilience Authentication Mechanism for Intelligent Healthcare System. IEEE Transactions on Industrial Informatics 2023;19(1):830-840.
36. Mijwil M, Omega John U, Youssef F, Indu B, Humam A-S. Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. Mesopotamian Journal of CyberSecurity 2023;2023:57-63.
37. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum 2022;3(12):e224873.
38. Wright A, Aaron S, Bates DW. The Big Phish: Cyberattacks Against U.S. Healthcare Systems. J Gen Intern Med 2016;31(10):1115-1118.
39. Latif R, Abbas H, Assar S. Distributed denial of service (DDoS) attack in cloud- assisted wireless body area networks: a systematic literature review. J Med Syst 2014;38(11):128.
40. Lee I. Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. Information 2022;13(9):404.
41. Slayton TB. Ransomware: The Virus Attacking the Healthcare Industry. J Leg Med 2018;38(2):287-311.
42. Rawat R, Mahor V, Garg B, Chouhan M, Pachlasiya K, Telang S. Chapter Fifteen - Modeling of cyber threat analysis and vulnerability in IoT-based healthcare systems during COVID. In: Kaklauskas A, Abraham A, Okoye K, Guggari S, editors. Lessons from COVID-19: Academic Press; 2022, p. 405-425.
43. Jadhav JS, Deshmukh J. A review study of the blockchain-based healthcare supply chain. Social Sciences & Humanities Open 2022;6(1):100328.
44. Chernyshev M, Zeadally S, Baig Z. Healthcare Data Breaches: Implications for Digital Forensic Readiness. J Med Syst 2018;43(1):7.
45. Sharma K. Internet of healthcare things security

vulnerabilities and jamming attack analysis. Expert Systems 2022;39(3):e12853.

46. Luo E, Bhuiyan M, Wang G, Rahman MA, Wu J, Atiquzzaman M. PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems. IEEE Communications Magazine 2018;56:163-168.
47. Shihab S, Altawy R. Lightweight Authentication Scheme for Healthcare With Robustness to Desynchronization Attacks. IEEE Internet of Things Journal 2023;PP:1-1.
48. Khan F, Al-Atawi AA, Alomari A, Alsirhani A, Alshahrani MM, Khan J, et al. Development of a Model for Spoofing Attacks in Internet of Things. Mathematics 2022;10(19):3686.
49. Iqbal M, Matulevičius R. Exploring sybil and double-spending risks in blockchain systems. IEEE Access 2021;9:76153-76177.
50. Lin X, Lu R, Shen X, Nemoto Y, Kato N. Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. IEEE Journal on Selected Areas in Communications 2009;27(4):365-378.
51. Kumar M, Raj H, Chaurasia N, Gill SS. Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. Internet of Things and Cyber-Physical Systems 2023;3:309-322.
52. Yang B, Cheng B, Liu Y, Wang L. Deep learning-enabled block scrambling algorithm for securing telemedicine data of table tennis players. Neural Computing and Applications 2021;35:1-14.
53. Shinde R, Patil S, Kotecha K, Potdar V, Selvachandran G, Abraham A. Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. Transactions on Emerging Telecommunications Technologies 2024;35(1):e4884.
54. Anderson C, Baskerville R, Kaul M. Managing compliance with privacy regulations through translation guardrails: A health information exchange case study. Information and Organization 2023;33(1):100455.
55. Azeez NA, der Vyver CV. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal 2019;20(2):97-108.
56. Butpheng C, Yeh K-H, Xiong H. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry 2020;12(7):1191.
57. Philip N, Rodrigues J, Wang H, Fong S, Chen J. Internet of Things for In-Home Health Monitoring Systems: Current Advances, Challenges and Future Directions. IEEE Journal on Selected Areas in Communications 2021;39:300-310.
58. Winker MA, Flanagin A, Chi-Lum B, White J, Andrews K, Kennett RL, et al. Guidelines for medical and health information sites on the internet: principles governing AMA web sites. American Medical Association. Jama 2000;283(12):1600-1606.
59. Yüksel B, Küpçü A, Ozkasap O. Research issues for privacy and security of electronic health services. Future Generation Computer Systems 2016;68
60. Juma M, Alattar F, Touqan B. Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB). IoT 2023;4(1):27-55.
61. Gong Y, Liu G, Xue Y, Li R, Meng L. A survey on dataset quality in machine learning. Information and Software Technology 2023;162:107268.
62. Srinivasan S, Deepalakshmi P. ENetRM: ElasticNet Regression Model based malicious cyber-attacks prediction in real-time server. Measurement: Sensors 2023;25:100654.
63. Omotunde H, R. Mouhamed M. The Modern Impact of Artificial Intelligence Systems in Healthcare: A Concise Analysis. Mesopotamian Journal of Artificial Intelligence in Healthcare 2023;2023:66-70.
64. Shaikh TA, Rasool T, Verma P. Machine

intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions. Artif Intell Med 2023;146:102692.

65. Sun Y, Lo F, Lo B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. IEEE Access 2019;PP:1-1.
66. D'Aniello G, Gravina R, Gaeta M, Fortino G. Situation-Aware Sensor-Based Wearable Computing Systems: A Reference Architecture-Driven Review. IEEE Sensors Journal 2022:1-1.
67. El Jaouhari S, Bouvet E. Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. Internet of Things 2022;18:100508.
68. Halder S, Ghosal A, Conti M. Secure over-the-air software updates in connected vehicles: A survey. Computer Networks 2020;178:107343.
69. La Manna M, Treccozzi L, Perazzo P, Saponara S, Dini G. Performance Evaluation of Attribute-Based Encryption in Automotive Embedded Platform for Secure Software Over-The-Air Update. Sensors 2021;21(2):515.
70. Benneh Mensah G, M. Mijwil M, Abotaleb M, Badr A, Adamopoulos I, S. Arafat A, et al. Role of Food and Drugs Authority Act, 1992 (PNDCL 305B) and Legislative Instrument (LI) in Regulating Artificial Intelligence Based Medical Devices, Apps, and Systems to Prevent Negligence. Babylonian Journal of Internet of Things 2024;2024:27-32.
71. Toor AA, Usman M, Younas F, M. Fong AC, Khan SA, Fong S. Mining Massive E-Health Data Streams for IoMT Enabled Healthcare Systems. Sensors 2020;20(7):2131.
72. Razdan S, Sharma S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. IETE Technical Review 2022;39(4):775-788.
73. Safitra MF, Lubis M, Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability 2023;15(18):13369.
74. Gravina R, Alinia P, Ghasemzadeh H, Fortino G. Multi-Sensor Fusion in Body Sensor Networks: State-of-the-art and research challenges. Information Fusion 2016;35
75. Hinga S, Imoize A, Ajani T, Atayero A. A Bird's Eye View of Near Field Communication Technology: Applications, Global Adoption, and Impact in Africa. SN Computer Science 2024;5
76. Lin K, Chen H, Li Z, Yan N, Xue H, Xia F. Efficiently Identifying Unknown COTS RFID Tags for Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems 2023;PP:1-11.
77. Sallam M. ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns. Healthcare 2023;11(6):887.
78. Alowais SA, Alghamdi SS, Alsuhebany N, Alqahtani T, Alshaya AI, Almohareb SN, et al. Revolutionizing healthcare: the role of artificial intelligence in clinical practice. BMC Medical Education 2023;23(1):689.
79. Sallam M, Mousa D. Evaluating ChatGPT performance in Arabic dialects: A comparative study showing defects in responding to Jordanian and Tunisian general health prompts. Mesopotamian Journal of Artificial Intelligence in Healthcare 2024;2024:1-7.
80. Sallam M, Al-Farajat A, Egger J. Envisioning the Future of ChatGPT in Healthcare: Insights and Recommendations from a Systematic Identification of Influential Research and a Call for Papers. Jordan Medical Journal 2024;58(1)
81. Mijwil M, Doshi R, Hiran K, Bala I, Guma ALI. The Effect of Human-Computer Interaction on New Applications by Exploring the Use Case of ChatGPT in Healthcare Services. 2024, p. 74-87.
82. Yamin MM, Ullah M, Ullah H, Katt B. Weaponized AI for cyber attacks. Journal of Information Security and Applications 2021;57:102722.
83. Chen Y, Esmaeilzadeh P. Generative AI in Medical

Practice: In-Depth Exploration of Privacy and Security Challenges. J Med Internet Res 2024;26:e53008.

84. Kaur R, Gabrijelčič D, Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion 2023;97:101804.
85. Yang J, Chen Y-L, Por LY, Ku CS. A Systematic Literature Review of Information Security in Chatbots. Applied Sciences 2023;13(11):6355.
86. Jerry-Egemba N. Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. Healthcare Management Forum 2023;37(1):21-25.
87. Molina SB, Nespoli P, Mármol FG. Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision. arXiv preprint arXiv:2312.06229 2023
88. Aljanabi M, Salman SA, Mijwil MM, Mohialden YM, Hussien NM, Abotaleb M, et al. Enhancing Security and Privacy in Healthcare with Generative AI-Based Detection and Mitigation of Data Poisoning Attacks software. Jordan Medical Journal 2024; In press

ضمان الامن والخصوصيه في انظمة الرعايه الصحيه: مراجعه تستكشف التحديات، الحلول، الاتجاهات المستقبليه والاستخدامات العمليه للذكاء الاصطناعي

إندو بالا[1]، عرفان أحمد بيندو[2]، معد محسن مجول[3]، مصطفى أبوطالب[4]، ووانغ يوندونغ[5]

[1]SEEE، جامعة لافلي المهنية، البنجاب، الهند

[2]RDC، جامعة لافلي المهنية، البنجاب، الهند

[3]قسم هندسة تقنيات الحاسوب، كلية بغداد للعلوم الاقتصادية الجامعة، العراق

[4]قسم برمجة النظم، جامعة جنوب الأورال الحكومية، روسيا

[5]معهد الإعلام والعلوم الاجتماعية والإنسانية، جامعة جنوب الأورال الحكومية، تشيليابينسك، روسيا

الملخص

الخلفية والأهداف: يعرض الهيكل المعقد لنظام الرعاية الصحية تحديات فريدة في ضمان الأمن والخصوصية. تهدف هذه المراجعة إلى البحث في هذه التحديات في سياق التكامل المتزايد للذكاء الاصطناعي (AI) في عمليات الرعاية الصحية.

منهجية الدراسة قمنا بإجراء تحليلٍ عميق لبنية نظام الرعاية الصحية، مع التركيز على ضرورة فهم طبيعته المتعددة الأوجه لحماية البيانات الحساسة بشكل فعال. قمنا بعد ذلك بتقييم المخاطر ونقاط الضعف المحتملة من خلال مراجعة الهجمات الإلكترونية السابقة التي استهدفت مؤسسات الرعاية الصحية ووضع أساس لاقتراح تدابير مضادة قوية.

النتائج: سلطت النتائج الضوء على الأهمية الحساسة لحماية بيانات الرعاية الصحية وتفاصيل طبيعة التهديدات التي يواجهها النظام. ومن خلال فحص الحوادث السابقة، حددنا مواطن الضعف الشائعة والأساليب التي تم من خلالها استغلال النظام. بناءً على هذه الأفكار، تم اقتراح استراتيجيات جديدة تهدف إلى التقليل من تأثير هذه الاختراقات الأمنية في سياق الرعاية الصحية.

الاستنتاجات: يقدم دمج الذكاء الاصطناعي مع الرعاية الصحية فرصاً ولكنه يفرض تحديات للأمن والخصوصية. تناولت هذه المراجعة العقبات التي يواجهها الباحثون في تأكيد أن تطبيقات الذكاء الاصطناعي في الرعاية الصحية آمنة وتحترم خصوصية المريض. أكدنا على الحاجة الى التكيف والتحسين المستمر لمواكبة التهديدات الناشئة. يعد ضمان أمان وخصوصية أنظمة الرعاية الصحية في عصر الذكاء الاصطناعي أمراً ملحاً. حددت هذه المراجعة التعقيدات التي ينطوي عليها ضمان أمن وخصوصية أنظمة الرعاية الصحية وحددت استراتيجيات استباقية لتعزيز مرونة مؤسسات الرعاية الصحية ضد التهديدات السيبرانية. إن البحث المستمر يعد أمراً ضرورياً لاستباق التحديات الأمنية المحتملة.

الكلمات الدالة: نظام الرعاية الصحية، الهجمات الإلكترونية، الأمن والخصوصية، التحديات.