Mesopotamian journal of Cybersecurity
Vol.4 No.2, **pp**. 20–62
DOI: https://doi.org/10.58496/MJCS/2024/006; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles

Guma Ali[1,3*], Maad M. Mijwil[2]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[2] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[3] *Department of Computer Science, Faculty of Science, Islamic University in Uganda, Arua Campus, Uganda*

ARTICLE INFO

Article History
Received 28 Feb 2024
Accepted 01 May 2024
Published 23 May 2024

Keywords
Healthcare
Smart healthcare
Emerging technologies
Cybersecre threats
Security mechanisms

ABSTRACT

Cutting-edge technologies have been widely employed in healthcare delivery, resulting in transformative advances and promising enhanced patient care, operational efficiency, and resource usage. However, the proliferation of networked devices and data-driven systems has created new cybersecurity threats that jeopardize the integrity, confidentiality, and availability of critical healthcare data. This review paper offers a comprehensive evaluation of the current state of cybersecurity in the context of smart healthcare, presenting a structured taxonomy of its existing cyber threats, mechanisms and essential roles. This study explored cybersecurity and smart healthcare systems (SHSs). It identified and discussed the most pressing cyber threats and attacks that SHSs face, including fake base stations, medjacking, and Sybil attacks. This study examined the security measures deployed to combat cyber threats and attacks in SHSs. These measures include cryptographic-based techniques, digital watermarking, digital steganography, and many others. Patient data protection, the prevention of data breaches, and the maintenance of SHS integrity and availability are some of the roles of cybersecurity in ensuring sustainable smart healthcare. The long-term viability of smart healthcare depends on the constant assessment of cyber risks that harm healthcare providers, patients, and professionals. This review aims to inform policymakers, healthcare practitioners, and technology stakeholders about the critical imperatives and best practices for fostering a secure and resilient smart healthcare ecosystem by synthesizing insights from multidisciplinary perspectives, such as cybersecurity, healthcare management, and sustainability research. Understanding the most recent cybersecurity measures is critical for controlling escalating cyber threats and attacks on SHSs and networks and encouraging intelligent healthcare delivery.

1. INTRODUCTION

The rapid global increase in the elderly population has led to a significant increase in the prevalence of chronic diseases such as cardiovascular diseases, diabetes, chronic respiratory diseases, cancer, heart failure, chronic kidney disease, hypertension, neurological disorders, asthma, autoimmune diseases, and osteoarthritis, which has resulted in high demand for medical services from traditional healthcare systems. The global shortage of health professionals, coupled with the advancement of emerging technologies, has given help to the healthcare industry, thus giving rise to smart healthcare [1][2]. Wells and Usman [3] and Bu et al. [4] defined smart healthcare as a healthcare system that integrates and uses various emerging technologies to monitor patients and instantly access their medical information remotely, connect healthcare stakeholders, and automatically diagnose and detect diseases at an early stage. In SHSs, wearable or nonwearable sensors are implanted in patients to monitor and collect physiological data such as cardiac activity, pulse rate, blood pressure, electrocardiogram, temperature, heart rate, respiratory rate, oxygen volume in the body, activity level, and brain waves, which help in monitoring patients' health conditions or environmental data such as air quality, temperature, humidity, etc. [5]. These physiological data and patient profiles form electronic health records, which are stored in the cloud to form medical cloud data that can be easily shared among patients, health professionals, medical institutions, and other stakeholders to meet the medical ecosystem's needs and for easy decision-making and resource allocations [6]. Smart healthcare systems have been developed to enable real-time patient monitoring, personalized patient treatment, real-time medical data analysis, telemedicine consultations, improving patient outcomes by utilizing available resources, ambient control and wellness, and safe and efficient patient data management [7][8].

*Corresponding author. Email: a.guma@muni.ac.ug

A report by Statista indicated that the revenue generated from the digital health market is expected to reach US$193.70 billion by 2024, the market size is estimated to grow by 9.16% (CAGR 2024-2028) annually, and by 2028, the market volume is projected to reach US$275.00 billion. Digital fitness and well-being will generate total revenue of US$93.56 billion by 2024 [9]. Figure 1 shows the market value trend for digital health.

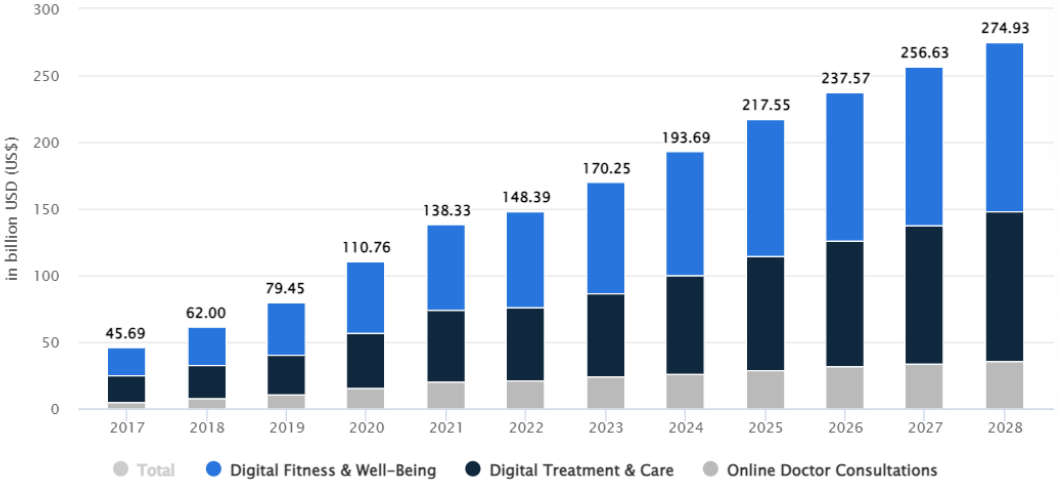

Fig. 1. The estimated market volume of digital health by 2028 ([21]).

The healthcare sector has transformed from healthcare 1.0 to healthcare 5.0, with different technologies used in each stage. Healthcare 1.0 (predigital era) was established between 1970 and 1990, healthcare 2.0 (digitization era) was from 1991 to 2005, the healthcare 3.0 era was established between 2006 and 2015, the healthcare 4.0 era was established between 2016 and 2019, and the era of healthcare 5.0 was established between 2020 and the present [10-12].

Smart healthcare architecture involves integrating cutting-edge and intelligent technologies into the design and infrastructure of healthcare facilities to increase the overall efficiency, effectiveness, and quality of healthcare services. It consists of (1) a perception or sensor layer, (2) a network layer, (3) an edge computing layer, (4) a fog computing layer, (5) a gateway layer, (6) a cloud computing layer, (7) a blockchain layer, (8) a data analytics layer, (9) a security layer, (10) an application layer, and (11) a regulatory layer. These layers support various functions, such as gathering medical data from patients using sensors and wearable devices, protecting medical data, storing data, analyzing data, and visualizing data by patients and healthcare professionals [10-12]. A wide range of emerging digital technologies, such as sensors and wearable technology, the internet of things (IoT), cloud computing, fog computing, edge computing, blockchain technology, drone technology, robotics, quantum computing, fifth-generation (5G) communication technology, three-dimensional (3D) printing and scanning, big data, nanotechnology, artificial intelligence, machine learning, deep learning, computer vision, tactile internet/haptics, virtual reality, augmented reality, and mixed reality, are used to successfully implement SHS [13-16]. These technologies have revolutionized healthcare services by offering essential services such as (1) real-time continuous patient remote monitoring and tracking, (2) telemedicine, (3) ambient assisted living, (4) smart self-management, (5) smart treatment reminders, compliance, and adherence, (6) personalized and connected healthcare, (7) disease diagnosis and treatment, (8) health management, (9) disease prevention and risk monitoring, (10) virtual assistants, (11) smart hospital management, (12) assisting drug research, (13) smart ambulances, (14) telesurgery, (15) virtual reality therapy, (16) predictive analytics, and (17) electronic health records [17-19]. The integration of smart technologies has revolutionized patient care and operational efficiency in the ever-evolving healthcare landscape. Amidst this transformation, cybersecurity has emerged as a critical facet, ensuring the integrity, confidentiality, and availability of sensitive healthcare data and systems. As we navigate toward sustainable healthcare ecosystems characterized by interconnected devices and data-driven decision-making, robust cybersecurity measures become increasingly paramount. The convergence of healthcare and digital technology offers unparalleled benefits, such as efficient and real-time patient monitoring, remote patient diagnosis, reduced treatment costs, efficient healthcare services with more accurate results, accessibility to medical services, streamlined healthcare operations, a secure medical platform, improved productivity, increased patient satisfaction, enhanced patient–doctor communication, predictive analytics, and improved decision-making [20-23].

Despite the tremendous benefits of SHSs, there has been an increase in cybersecurity threats and attacks to implanted, wearable, and non-wearable medical devices that generate and store sensitive patient information. Some of the common cyber threats and attacks in smart healthcare include healthcare data breaches, privacy concerns, denial-of-service (DoS) and distributed DoS (DDoS) attacks, ransomware, phishing attacks, eavesdropping attacks, man-in-the-middle attacks, impersonation attacks, insider threats, replay attacks, medical identity thefts, brute-force attacks, fake base stations, supply

chain attacks, medjacking, advanced persistent threats, SQL injection attacks, legacy systems, side-channel attacks, jamming attacks, buffer overflow, Sybil attacks, routing attacks, cross-site scripting attacks, cross-site request forgery attacks, session hijacking attacks, account hijacking, cookie manipulation attacks, sensor attacks, tampering attacks, zero-day vulnerabilities, cryptographic attacks, stolen physical smart device attacks, cloud-based threats, medical IoT device vulnerabilities, attacks associated with blockchain, evasion attacks, poisoning attacks, extraction attacks/model stealing/model inversion, and regulatory compliance challenges [24-29]. These attacks target patients' health information, financial information (e.g., credit card and bank account numbers), patients' identifying information (e.g., social security numbers), and medical research and innovation intellectual property, thus compromising privacy, confidentiality, access control, integrity, authentication, nonrepudiation, anonymity, and availability [30-32]. Between March 2022 and March 2023, data breaches in the healthcare industry cost nearly US$11 million [33]. These cyber threats and attacks result in financial loss, reputational damage, legal consequences, fraudulent misuse of patient information, loss of access to critical SHSs, and loss of patient trust.

Robust cybersecurity in smart healthcare applications is vital for safeguarding sensitive patient information and privacy [34]. Best security practices and protocols, such as cryptographic-based techniques, digital watermarking, pseudonymization-based techniques, digital signature-based solutions, key management-based solutions, anonymization, authentication-based techniques, access control-based techniques, blockchain and cloud-based privacy preservation techniques, IoT security, backup and recovery, network security, endpoint security, education and training, incident response plans, continuous monitoring, regular security audits, network segmentation, and regulatory compliance, contribute to the security of smart healthcare applications and systems [35-37]. According to Statista, by 2026, the global expenditure on cybersecurity in the healthcare industry is estimated to surpass US$27.39 billion, and by 2030, the global cybersecurity market in the healthcare sector will exceed US$58 billion, increasing with an annual compound growth rate of 14% [38]. This is because cybercriminals target the healthcare sector, forcing governments and healthcare organizations to adopt cybersecurity practices to ensure patient safety and privacy [38]. Cybersecurity plays a significant role in ensuring the sustainability and effectiveness of smart healthcare systems because it protects patient data, prevents cyberattacks, maintains healthcare stakeholder trust and confidence, ensures continuity of care, complies with regulations, facilitates healthcare innovation, prevents data breaches, maintains SHS integrity and availability, protects patient privacy, manages vendor risk, ensures smart healthcare network security, user identity and access management, protects telehealth and smart devices, and ensures healthcare software development, incident response, continuous monitoring, and interoperability security [39][40].

Several reviews have been published on the role of cybersecurity in sustainable smart healthcare. However, to our knowledge, no state-of-the-art review has thoroughly described cyber threats, effective cybersecurity techniques, or the role of cybersecurity in ensuring sustainable smart healthcare. This study, therefore, aims to present a state-of-the-art review on cybersecurity for sustainable smart healthcare. This review helps to further the knowledge of the link between cybersecurity, sustainability, and smart healthcare while providing practical insights for policymakers, healthcare practitioners, and cybersecurity experts. The major objectives and contributions of this review include the following:

- To explore cybersecurity and SHSs.
- To identify the existing cyber threats in SHSs and networks.
- To discuss the different security mechanisms used to combat cyber threats in SHSs.
- To examine the role of cybersecurity in sustaining smart healthcare.

The significance and implications of this review paper are multifaceted and critical for healthcare and technology integration. They include identifying and addressing cyber threats, promoting sustainability in healthcare practices, guiding policy and practice, encouraging collaboration and innovation, and emphasizing the human element in cybersecurity. It also has several limitations, such as its scope, limited time, publication bias, source quality, generalizability, language bias, intrinsic subjectivity, and changing nature.

The remainder of the paper is organized as follows. The materials and methods are described in Section 2. The third section covers cybersecurity and SHSs, while Section 4 presents the existing cyber threats in the smart healthcare ecosystem, security mechanisms in SHSs are explored in Section 5, the role of cybersecurity in sustaining smart healthcare is explored in Section 6, and Section 7 covers the conclusions.

2. MATERIALS AND METHODS

In this research, the authors conducted a state-of-the-art review investigating cybersecurity for sustainable smart healthcare. The integrative literature method was used in this research. The review gathered and evaluated literature from journal articles, conference proceedings and workshops, book chapters, magazines, and websites. This study examined the literature published between 2020 and 2024 to validate the most recent breakthroughs in smart healthcare. Using relevant keywords, the researchers collected literature from academic search engines and databases, including Nature, PLOS ONE,

ACM Digital Library, National Library of Medicine, Frontiers, Wiley Online Library, SAGE, Taylor & Francis, Hindawi, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, IGI Global, and Google Scholar.

The researchers first screened the relevant literature using the title, abstract, and keywords to validate its relevance and then extensively analyzed the selected literature to extract useful information for the study. Keywords such as 'Healthcare' OR 'smart healthcare' OR 'intelligent healthcare' OR 'SHS' OR 'history of healthcare' OR 'evolution of healthcare' OR 'smart healthcare architecture' OR 'emerging technologies in smart healthcare' OR 'healthcare services in smart healthcare' AND 'cyber threats in smart healthcare' OR 'cyber-attacks in smart healthcare' OR 'cybersecurity' OR 'security requirements in smart healthcare' AND 'security mechanisms in smart healthcare' OR 'mitigation measures for cyber threats in smart healthcare' were used to retrieve the relevant literature.

Several steps are involved in this state-of-the-art review process: (1) over 1000 publications were identified from the academic search engines and databases; (2) the number of publications was reduced to 700 after the screening of the abstract and removal of the duplicates; (3) after assessing the eligibility, the total number of publications decreased to 550; and (4) finally, the total number of relevant publications that met the criteria was 199 and were included in the study. The research papers were chosen based on their relevance, methodological rigour, clarity and coherence, validity and reliability, peer review process, credibility of sources, bias and confounding variables, timeliness and relevance, citations and references, and synthesis of findings. Researchers employed these factors to properly analyze the quality of research papers used in literature reviews, ensuring the validity and dependability of the research findings. Figure 2 depicts the digital libraries used to retrieve the selected research papers for this review.

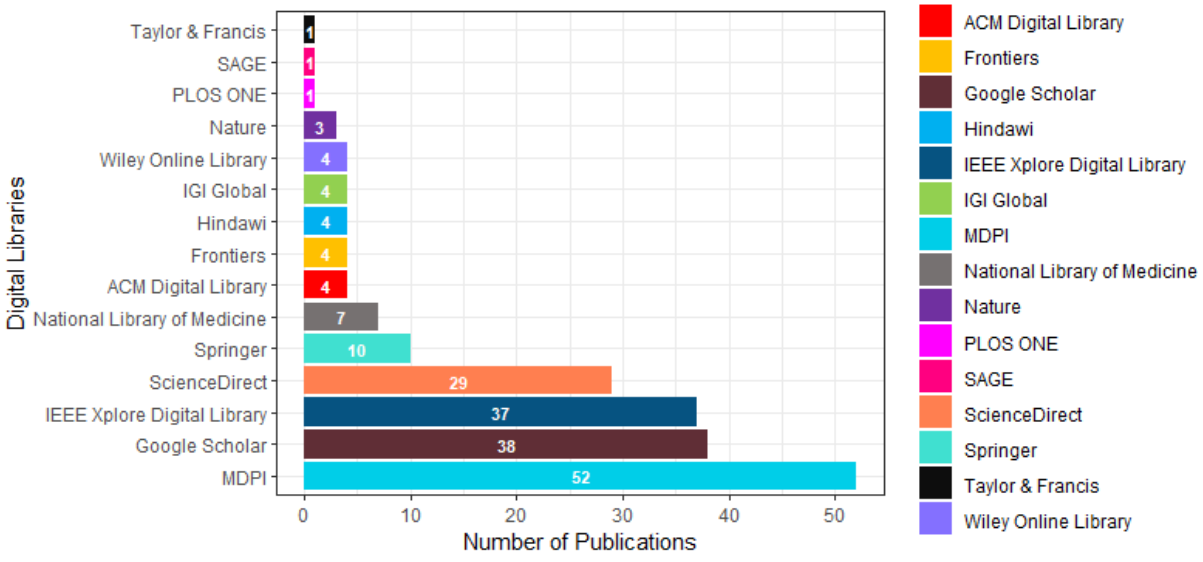

Fig. 2. The digital libraries used to retrieve the selected research papers for this review are shown.

Figure 3 shows the distribution of research paper sources based on digital libraries.

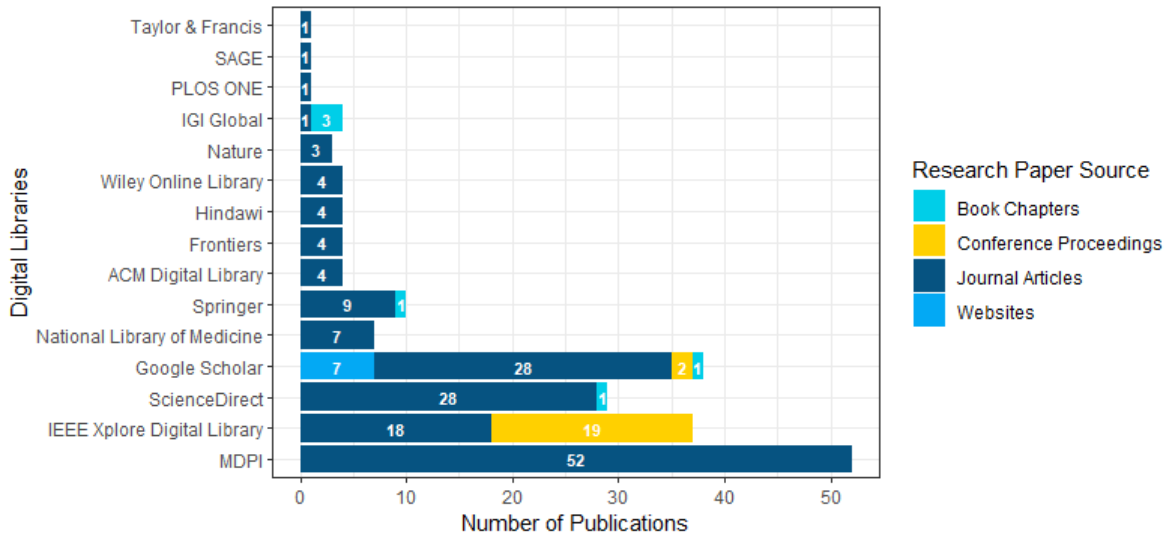

Fig. 3. The distribution of research paper sources based on digital libraries.

Figure 4 depicts the distribution of selected papers by digital libraries based on the year of publication.

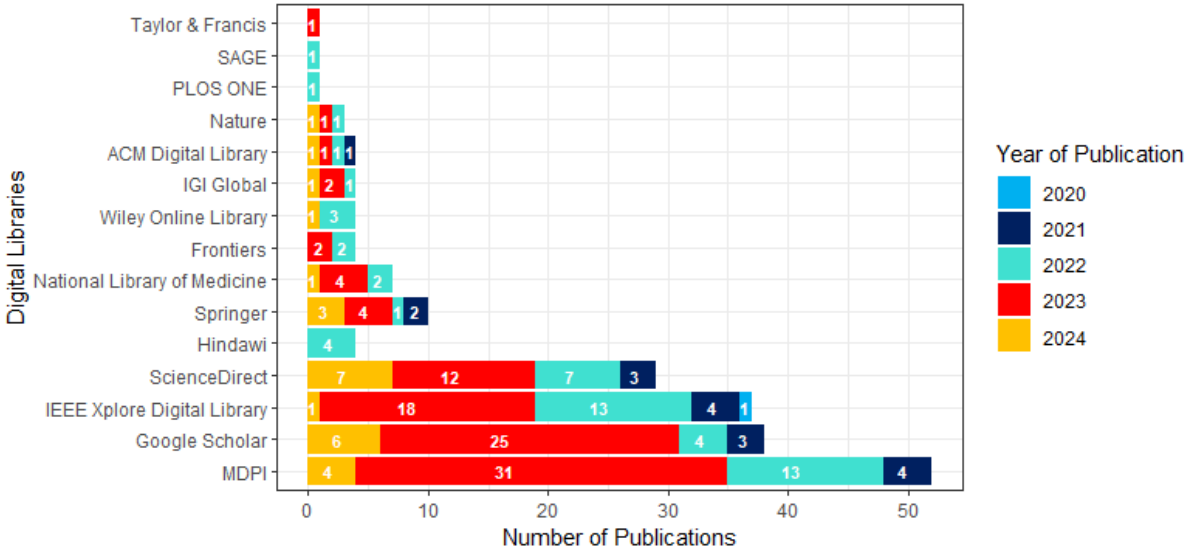

Fig. 4. The distribution of selected papers by digital library based on the year of publication.

The inclusion and exclusion criteria were used to select relevant review material. A test-retest approach was used to prevent biases in exclusion criteria, where the retrieved papers were reviewed multiple times for accuracy after being selected randomly from the original research. Other strategies for addressing or mitigating potential biases during the literature review process include applying comprehensive search strategies, transparent reporting, peer review, critical appraisal, sensitivity analyses, conflict of interest disclosure, meta-analysis, applying various perspectives, and ongoing monitoring. The researchers followed steps such as clearly defining the inclusion and exclusion criteria, a comprehensive search strategy, a systematic approach, independent reviewers, critical appraisal of studies, publication bias assessment, transparent reporting, sensitivity analysis, confounding factor consideration, and peer review to minimize biases in the review and improve the credibility of the review findings. Table I illustrates the inclusion and exclusion criteria for selecting relevant material for the study.

TABLE I. THE INCLUSION AND EXCLUSION CRITERIA FOR SELECTING RELEVANT MATERIAL FOR REVIEW ARE ILLUSTRATED.

Inclusion Criteria	Exclusion Criteria
Studies related to smart healthcare	Studies not related to smart healthcare.
Research papers written in English	Research papers not written in English.

Research papers related to cyber threats in the smart healthcare ecosystem	Research papers without results and reasonable research contributions
Research papers related to security mechanisms in smart healthcare	Research studies whose content lacks relevance, originality, and impact
Research papers published between January 2020 and April 2024	Smart healthcare studies published before January 2020
Research papers that are scientific, relevant, and capable of answering the research questions	

The researchers used thematic analysis to extract and evaluate the key findings from each research paper chosen for the review. The researchers analyzed and discussed cybersecurity and SHSs, cyber threats in SHSs, security mechanisms in SHSs, and the role of cybersecurity in sustaining smart healthcare. The researchers feel that the study provides valuable insights into the current state of the smart healthcare domain and may be used as a reference for future research.

3. CYBERSECURITY AND SHS: AN OVERVIEW

The use of cybercrimes in healthcare organizations is increasing due to the sensitivity of patient and healthcare data, which has adverse effects. These cyber threats are prevalent owing to an overreliance on smart technologies such as wearable, implantable, digestive, and biomedical sensors; smart devices; healthcare mobile applications; and smart medical equipment to improve healthcare services. As a result, designing, implementing, and investing in solid cybersecurity measures is critical for smart healthcare networks reacting to rising cyber threats [41]. According to Mijwil et al. [42], cybersecurity in smart healthcare is an action, strategy, practice, technology, or procedure taken by healthcare organizations to protect their technological assets from cyber-attacks, unauthorized access, use, disclosure, or disruption of healthcare services to ensure the confidentiality, integrity, and availability of healthcare information. In SHSs, cybersecurity technologies help to protect smart healthcare devices (e.g., wearables, pacemakers, artificial pancreases), institutional images, sensitive patient data, medical records, legal compliance, and financial data from breaches and unauthorized access and possible misuse and to ensure healthcare business continuity [7][41]. Cybersecurity ensures communication, ensures healthcare user authentication and authorization, helps in risk analysis and management, prevents attacks and medical fraud, offers high-quality patient care, protects healthcare networks, handles multifaceted treatments with outstanding patient care, safeguards healthcare access, enhances healthcare services and outcomes, improves daily healthcare activities, and coordinates and controls the process of treatment [43]. It has also been applied in network security, application security, information security, operational security, disaster recovery and operational continuity, and end-user training [44]. For reliable and trusted healthcare information sharing, cybersecurity principles (e.g., privacy, confidentiality, integrity, availability, authenticity, auditing, nonrepudiation, secure data transmission, and access control) must be met [41].

To ensure healthcare information security, SHSs must comply with security requirements and apply suitable protection mechanisms. Some cybersecurity requirements for smart healthcare are briefly discussed below [45-47].

- *Confidentiality* is a security requirement that guarantees that only authorized entities (such as healthcare professionals and patients) can access sensitive medical information, IoMT devices, and smart medical equipment. In the SHS, sensitive medical data are collected from the IoMT and wireless body area networks and are kept secret, whether in transit or storage. Only authorized entities such as healthcare professionals and personnel can access it. Patients may only trust physicians and other healthcare providers if their sensitive information is kept secret. Encryption and access control mechanisms safeguard the security of healthcare data during storage and transit and protect against illegal access.
- *Integrity* is a security principle that ensures that a patient's medical information is accurate, reliable, and comprehensive. This ensures that no unauthorized entities delete, destroy, corrupt, change, or manipulate medical data during the end-to-end transmission between SHS and IoMT devices. Integrity is vital because IoMT devices collect patient data and store it in an SHS, which physicians use to treat patients and prescribe medication. Such acquired patient data must be accurate and consistent, as altered medical records might endanger human health. As a result, transmitted healthcare data must be validated against manipulation, unlawful change, and deletion by adversaries, as well as inadvertent communication failures during transmission or storage, which can lead to misdiagnosis or incorrect prescriptions. Furthermore, medical data should not be added or withdrawn from SHSs without authority. Cryptographic algorithms such as the Secure Hash Algorithm (SHA)-256, Advanced Encryption Standard (AES)128/256, and S-box are used to protect data integrity.
- *Availability* is a security principle that ensures that smart healthcare services and resources are available or accessible to legitimate healthcare users when needed, including during system failures or attacks. It guarantees that authorized healthcare users have continual and dependable access to medical information, IoMT devices, and SHSs, independent of their location or time. This attribute guarantees that healthcare personnel can access patient healthcare data to perform procedures and treatments and that the IoMT, medical devices, communication networks, and SHS function accurately. Patients must be able to access their electronic healthcare records, and healthcare providers must utilize them to treat their patients. Furthermore, an SHS must ensure that correct medical data are available to authentic

healthcare users at all times and from any location. Furthermore, high-availability systems must prevent smart healthcare service disruptions and maintain the usefulness of healthcare records after HIPAA security and privacy regulations are applied.

- *Privacy* is essential in smart healthcare because it safeguards patients' medical secrets and personal data, which may only be shared after seeking consent. Patient privacy information, including facts on infectious illnesses, sexual orientation, mental health, drug addiction, and identity, is deemed vital and sensitive and must not be disclosed to unauthorized users, even if intercepted. Smart healthcare systems must treat patients' data in a lawful, just, and transparent manner for an explicit and legitimate goal because the data are sensitive, and there is a need to obtain patient consent. Medical images are typically labeled with patient IDs and histories, and they must be kept secure to prevent illegal access and abuse. Furthermore, no unauthorized user must identify patients, insurance providers, researchers, or management personnel, but physicians, nurses, and cashiers may utilize their information to undertake treatment and billing since privacy incorporates anonymity. Protecting healthcare users' privacy is critical in smart healthcare networks because cyber criminals can trace their identities and obtain sensitive healthcare and personal information. As a result, patients' and healthcare professionals' true identities must be protected in the smart healthcare network using data anonymization.
- *Authentication* in SHSs is the process of confirming the identities of entities (e.g., healthcare users, IoMT devices, servers, and gateways) and determining if they are who they claim to be before utilizing SHSs or resources. Authentication processes in the SHS can be device-to-device, healthcare user-to-device, or healthcare user-to-healthcare user, and they are necessary so that authenticated entities can communicate and perform actions such as accessing, modifying, or deleting sensitive medical information. This can be accomplished by implementing two-factor, multifactor, and robust authentication mechanisms that use knowledge, possession, inheritance, location, or behavior factors to authenticate healthcare users' identities before accessing SHSs and services. Authenticating smart devices, systems, or apps generates secure session keys that prove that healthcare data shared in smart healthcare networks are authorized. Healthcare personnel, patients, and IoMT devices must be validated before accessing SHSs to avoid forgeries and masquerade attacks. Smart healthcare system authentication is achieved by exchanging authentication keys, digital signatures, and certificates.
- *Authorization* in an SHS is the process of deciding whether verified entities have access rights and privileges to the SHS's resources, services, and healthcare data that they need to complete their tasks. In a secure smart healthcare network, entity permission comes after authentication to strengthen security and guard against healthcare threats. When the healthcare identity verification procedure is completed successfully, each entity is granted access rights or privileges to conduct tasks in the smart healthcare environment. In contrast to other health providers, a physician should have complete access to patient healthcare data. Smart healthcare systems use permission to manage access to sensitive patient information and ensure that authorized entities (IoMT devices) communicate sensitive healthcare data to others (healthcare professionals).
- *Accountability and auditability* are key security considerations in smart healthcare. Accountability is a cybersecurity principle that ensures that the actions of entities in an SHS can be traced back to them and that they are accountable for their actions related to the security and privacy of healthcare professionals and patient healthcare data. All healthcare information is recorded in an SHS, and every healthcare stakeholder must understand its role in safeguarding sensitive healthcare information by preventing unauthorized access to an SHS, sensitive healthcare information, or healthcare data breaches. This recorded healthcare information or logs can be used to identify healthcare users who conducted the acts or to trace IoMT devices in case of a security problem. On the other hand, auditing refers to an SHS's capacity to continuously record, track, and monitor healthcare user behaviors and examine and probe security measures to ensure compliance with legislation, industry standards, and best practices. Smart healthcare systems keep track of all healthcare user activities in chronological order, for example, system login time, access log maintenance, and data alteration, and healthcare users are held accountable for their actions while using SHSs and handling sensitive patient healthcare information. Smart healthcare auditing protects patient data, ensures the security and integrity of healthcare systems and devices, detects and monitors illegal access and disclosure of healthcare records, assesses vulnerabilities, and ensures regulatory and standard compliance.
- *Access control* is the process of regulating, restricting, or controlling access to SHSs, IoMT devices, sensitive patient data, or resources that can only be accessed by authorized entities. Healthcare users are assigned appropriate access levels based on their roles and responsibilities. The access control policy is based on each authorized healthcare professional's privileges and rights as granted by the patient or a trusted third party. Patients can manage those who have access to their sensitive healthcare records by providing consent. Role-based and attribute-based access controls are frequently used in SHSs and apps to protect sensitive patient data, maintain the integrity of IoMT devices, and ensure regulatory compliance with laws such as the HIPAA and the GDPR.
- *Nonrepudiation* in SHSs ensures that entities cannot deny carrying out acts inside the smart healthcare network, such as modifying patients' sensitive healthcare information or accessing sensitive data. Given the communication between two authorized entities in an SHS, the physician cannot deny treating the patient in the future, and the patient cannot deny receiving care from the physician because all acts are recorded in the SHS or patients and physicians cannot reject

the legitimacy of their signatures after misappropriating health information. Nonrepudiation allows healthcare users to prove the occurrence or nonoccurrence of an event. Because sensitive patient data and transactions are shared electronically, nonrepudiation contributes to authentication and authorization, data integrity, accountability and auditing, legal and regulatory compliance, and trust and confidence. Smart healthcare systems may achieve nonrepudiation by utilizing digital signatures, cryptographic hashing, secure communication protocols, robust access control, audit trails, and logging mechanisms.

- *Anonymity* refers to SHSs' capacity to conceal, mask, or protect the identities and personal information of healthcare users engaging in healthcare processes while effectively transmitting relevant healthcare data. Anonymizing healthcare data for a specific purpose and identifying patient and healthcare professional information allows anonymized data to be linked to their identities. Patients' identities, for example, can be anonymously kept in an SHS, preventing servers from learning their identities. Smart healthcare systems may evaluate and use healthcare data to enhance healthcare outcomes and decision-making while protecting patients' privacy and confidentiality. It protects sensitive patient data, ensures the integrity and trustworthiness of IoMT devices and smart healthcare environments, reduces the risk of unauthorized access or healthcare data breaches, secures communication and IoMT devices, and fosters trust among healthcare users and other stakeholders. Smart healthcare systems accomplish anonymity using data encryption, deidentification techniques, and secure communication protocols.
- *Reliability* refers to an SHS's ability to consistently deliver accurate and timely healthcare services while preserving the confidentiality, integrity, and accessibility of sensitive health data in the face of diverse smart healthcare networks, system and hardware failures, and numerous environmental conditions. Reliability is vital to smart healthcare networks when IoMT devices sense, collect and transmit healthcare data in high-risk environments. This guarantees that secure and trustworthy healthcare services are consistently delivered while preserving sensitive patient data and privacy.
- *Resiliency* is the ability of SHSs, IoMT devices, and processes to resist and adapt to challenges, disruptions, and unanticipated occurrences while maintaining their functionality and efficiency. Smart healthcare relies heavily on networked IoMT devices, networks, and healthcare data to deliver efficient and effective healthcare services. Smart healthcare and IoMT systems must evade and adapt to system outages, cyberattacks, natural catastrophes, and other emergencies without jeopardizing patient care or data security while safeguarding medical devices and healthcare information in the event of an attack. Resilient SHSs promote redundancy, robustness, flexibility, and adaptation to consistently provide high-quality healthcare and services, even under adverse situations. It ensures patient safety, privacy, and confidence in smart healthcare settings while protecting patient data and healthcare system confidentiality, integrity, and availability.
- *Fault tolerance* refers to an SHS's ability to continue functioning and provide healthcare services in the face of faults or failures caused by technological malfunctions, human errors, or malicious attacks. Most SHSs use and implement IoT, cloud computing, and big data analytics to enhance patient care, streamline healthcare operations, and increase efficiency. These technologies and systems may introduce susceptibilities that adversaries can exploit, posing various cybersecurity concerns. Fault tolerance requires that security services be provided by an SHS even when a defect exists. Smart healthcare providers who emphasize fault tolerance as a cybersecurity principle may increase system resilience, minimize possible risks, and assure continuous delivery of high-quality healthcare services while preserving patient healthcare data and privacy.
- *Robustness* refers to the ability of SHS and IoMT devices to maintain operation and performance despite various challenges, uncertainties, and adverse conditions. This ensures that an SHS can offer services accurately, quickly, and securely while effectively navigating the inherent challenges, uncertainties, cyber threats and assaults in healthcare contexts and retaining functionality and integrity. Smart healthcare systems implement robust security measures and adhere to regulations, industry standards, and best practices to minimize cybersecurity threats, secure sensitive healthcare information, and maintain security, integrity, and availability.
- *Freshness* refers to the ability of entities in smart healthcare to transmit new, up-to-date, relevant, and sensitive healthcare data promptly. Sensitive patient healthcare data, crucial SHSs, and IoMT devices are linked to smart healthcare networks, ensuring that healthcare data and systems are accurate and current for patient care, medical research, and decision-making processes. For instance, the physician must have the most recent patient's healthcare information, as storing obsolete information might lead to inconsistencies. Incorporating freshness into SHSs helps increase system resilience, protect patient data and essential healthcare infrastructure from cyber threats, ensure the integrity, confidentiality, and availability of healthcare data and services, and resist replay attacks.
- *Forward secrecy* in smart healthcare is a cryptographic technique that ensures that previous communications between SHSs, IoMT devices, patients, and healthcare professionals remain secure even if the encryption key used to encrypt the communications is compromised in the future. If an attacker illegally accesses the encryption key, they cannot decrypt past communications using the compromised decryption key. Forward secrecy is used in smart healthcare to ensure patient privacy, security, and patient data confidentiality and integrity by preserving previous conversations, adhering to healthcare regulations, and fostering stakeholder trust.

- *Backward secrecy* is a security requirement in SHSs that ensures that previous session keys and healthcare data remain confidential from newly added IoMT devices in an intelligent healthcare communication environment. Even if cybercriminals gain access to long-term private keys in the future, they should be unable to decrypt previous communications or access past healthcare data. Backward secrecy protects the confidentiality, integrity, privacy, and security of sensitive healthcare data in SHSs.
- *Revocation* is the process of cancelling or revoking access privileges or digital certificates for healthcare users, IoMT devices, or entities that are no longer authorized to access specific smart healthcare resources or systems. A patient can revoke approval for a healthcare professional to access his or her healthcare records. New access rights are immediately updated on the SHS, preventing healthcare professionals from accessing the information. This revocation of access rights for a particular healthcare professional should not interfere with the access rights granted to another, nor should it need the creation of new login credentials and cryptographic keys. As much as the privacy of healthcare professionals and patients is crucial, in the event of a disagreement, only trusted authorities must track the true identity of the healthcare professionals and patients and revoke the identities of the disobedient healthcare professionals and patients from the smart healthcare network. This security principle is essential when dealing with sensitive patient data and critical SHSs because it protects their confidentiality, privacy, and integrity by revoking access rights or digital certificates as soon as necessary. Figure 5 shows a summary of the cybersecurity requirements of an SHS.

Fig. 5. The cybersecurity requirements in smart healthcare

4. CASE STUDIES OF THE DEMONSTRATING REAL-WORLD APPLICATIONS OF SMART HEALTHCARE ARCHITECTURE

The practical applications of smart healthcare architecture in a hospital context include the following:

4.1 Remote patient monitoring

Patients with chronic diseases, such as diabetes or heart disease, are given intelligent wearable devices with sensors that monitor vital indicators, including heart rate, blood pressure, blood glucose, and activity levels. Wearable devices continually capture patient data and securely send it to a centralized healthcare platform via wireless connectivity, such as Bluetooth or Wi-Fi. A cloud-based healthcare platform uses advanced analytics and machine learning algorithms to process patient data. This platform can evaluate real-time data to identify abnormalities, trends, and patterns that might suggest future health concerns or crises. The healthcare platform includes a decision support system that uses collected data to deliver insights and suggestions to healthcare practitioners. For example, if a patient's blood glucose levels are persistently high, the system may recommend changing their prescription dose or lifestyle habits. The system may send warnings and

messages to healthcare practitioners, caregivers, and patients in the event of aberrant readings or crucial occurrences. These warnings can be delivered by mobile apps, text messages, or email, providing prompt intervention and monitoring [46].

4.2 Monitoring pregnancy

In-home self-monitoring, one of the essential components of prenatal healthcare, enables pregnant women to use pregnancy-related wearable technologies such as fetal monitors and multifunctional health screening tools to manage and monitor maternal health indicators such as blood pressure, fetal blood sugar, fetal heart rate, blood pressure, oxygenation, pulse, lipids, and electrocardiograms. These measurements are relayed wirelessly to a gateway, which stores and analyzes them on the cloud. Cloud computing allows a variety of apps to access these healthcare data, offering real-time health monitoring and guidance to doctors and pregnant mothers. These cutting-edge technologies significantly decrease the strain on medical and nursing personnel, enhance productivity, make it simpler for pregnant women to access healthcare, and elevate the grade of obstetric treatment [46].

4.3 Monitoring sports athletics

Wireless technologies, body sensors and fitness trackers in exercise spaces substantially influence life efficiency and health system reliability. Wearable devices are used to evaluate and analyze physiological considerations; advance health; enhance exercise compliance among diverse groups ranging from patients to expert athletes; and monitor heart rate, respiratory rate, and exercise rhythm continuously and instantly. The system uploads sensor data to the IoMT system's Ethernet module to establish the athlete's physical state, and the data are subsequently made available to the user over the internet. Fog computing services categorize a patient's health status as protected or at risk by processing incoming health data from every part of the model using the queue. This minimizes the amount of health data transported across the cloud, lowering the cost of computer resources and accurately predicting athletic anomalies [46].

5. EXISTING CYBER SECURITY THREATS IN THE SMART HEALTHCARE ECOSYSTEM

The confidential healthcare and financial data in SHSs require adequate security and privacy attention because they are vulnerable and targeted by cybercriminals. Cybersecurity threats in smart healthcare ecosystems are classified into seven (7) main categories: privacy attacks, confidentiality attacks, integrity attacks, availability attacks, authentication attacks, authorization attacks, and trustworthiness attacks. Figure 6 illustrates the taxonomy of cybersecurity threats in the smart healthcare ecosystem.

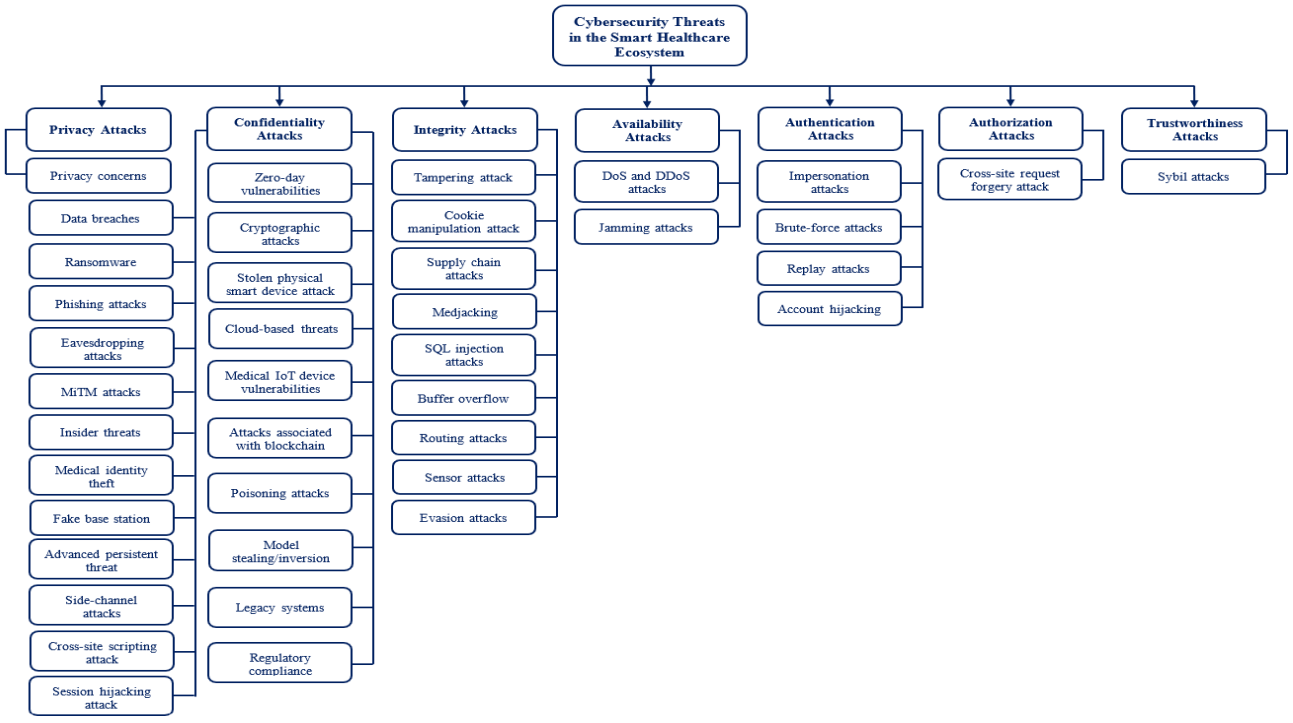

Fig. 6. Illustrates the taxonomy of cybersecurity threats in the smart healthcare ecosystem

5.1 Privacy Attacks

Cybersecurity threats to privacy include the following:

5.1.1 Privacy concerns

The emerging technologies in SHSs collect patients' sensitive healthcare data and vital parameters, which are stored in cloud databases for healthcare professionals to share and analyze. However, their security and privacy remain serious concerns [31]. Privacy in healthcare refers to protecting patients' healthcare data from unauthorized access, use, and disclosure to third parties. In SHS, patients' confidential healthcare and financial data are used, shared, and accessed by unauthorized people and parties such as the government, researchers, pharmaceutical companies, and laboratories, thus posing severe privacy issues [6]. When cybercriminals access sensitive healthcare data such as medical records, test results, and prescriptions, they can sell them on the dark web or black market [3]. The two most dangerous threats to patient data privacy are a lack of understanding of healthcare policies and regulations and hackers [48]. When individuals lose their smartphone, user ID and password used to access the SHS, there is a high risk that the privacy of the healthcare information stored in the smartphone may be compromised, leaked and shared with unauthorized people [2][37]. Collecting and recording patient private healthcare data in intelligent healthcare systems poses privacy issues. For example, some individuals prefer to limit what people in their private surroundings, such as family members, know about their health, possibly because they fear being evaluated, admonished, discriminated against, or even penalized for their physical and health status. Others may choose not to care for their family members due to their present health and may be reluctant to share their health condition with others due to a fear of social stigma [49].

5.2 Confidentiality Attacks

The existing cyber security threats against confidentiality include the following:

5.2.1 Healthcare data breaches

Health data breaches pose significant risks to patient privacy and healthcare system integrity because of inadequate security measures, interconnected systems, human error, malware, third-party vendors, legacy systems, insider threats, regulatory compliance challenges, lack of security awareness, and data monetization and theft [43]. A healthcare data breach is the unlawful use or exposure of sensitive healthcare information that compromises privacy and security. Smart healthcare systems collect sensitive healthcare and financial data from patients and store it on servers to be accessible to healthcare professionals and patients anytime and anywhere. These data can be accessed using smartphones and other smart devices, which can cause privacy breaches. These systems may have software vulnerabilities, security loopholes, and insecure databases, leading to the disclosure of confidential healthcare data. Health data breaches can be categorized as internal or external. Internal agents perpetrate internal healthcare data breaches by abusing their privileges, unauthorized access, and inappropriate disposal of sensitive data or sharing confidential healthcare data with unauthorized people. External healthcare data breaches are compromised by external parties performing hacking, malware attacks, unauthorized access, ransomware attacks, phishing attacks, and spyware. Medical data, which include a patient's medical history, diagnosis, treatments, and personal identifying information, are subject to breaches. Such breaches can have catastrophic repercussions, including identity theft, fraud, and medical misconduct [50]. The compromised healthcare data are highly valued on the dark web and black market [30]. According to a report by the Absolute Software Corporation, healthcare data breaches cost between US$250,000 and US$2.5 million [51].

5.2.2 Ransomware

Ransomware is one of the most severe cyber threats experienced by SHSs because of the value of stored healthcare data and the possibility of healthcare providers paying [52][53]. Ahmed et al. [54] and Al-Aboosi et al. [55] defined ransomware in healthcare as malware that encrypts critical patient data, blocks system and device access or disrupts healthcare services and demands a ransom payment in cryptocurrency in exchange for the decryption key known by the cybercriminal. During the COVID-19 pandemic, ransomware attacks increased significantly because of telemedicine. Cybercriminals use ransomware to infiltrate SHS. Once the system is infiltrated, it encrypts healthcare records, deactivates smart devices, and blocks SHSs, thus making smart devices, surgical instruments, and life support equipment inaccessible and inoperable to healthcare professionals and patients. The attackers then send messages to healthcare providers and patients demanding ransom in untraceable cryptocurrency for them to decrypt or regain access to their smart devices and healthcare records [32]. Ransomware is easily installed and spreads to cutting-edge devices through phishing emails [43]. Adversaries are providing ransomware-as-a-service on the dark web for others to use. Examples of Ransomware attacks in SHS include the following: (1) On March 3, 2024, a BlackCat ransomware organization ("ALPHV") launched a Ransomware attack against the U.S. healthcare company Change Healthcare. The attack encrypted their online systems and disrupted countrywide drug prescription services for weeks before demanding a ransom. Change Healthcare paid a US$22 million

ransom for a decryption key to prevent the BlackCat ransomware organization from releasing four terabytes of stolen data online. (2) On October 26, 2020, a Ryuk ransomware attack crippled the computer network systems of six hospital systems stretching from New York to California for 24 hours, rendering electronic health records unavailable, and in most hospitals, it lasted for weeks. The attackers utilized phishing emails to infect the hospitals' computer network systems with the BazarLoader malware, which was subsequently deployed via the Cobalt Strike pen-testing platform, giving the attackers further capacity to penetrate the network before distributing the Ryuk ransomware. The attackers targeted healthcare businesses to earn financially from ransom payments, and more than $1 million in ransom was paid by unnamed hospitals [56]. (3) On 11 January 2018, Hancock Regional Hospital in Greenfield, Indiana, was attacked with ransomware called SamSam. The ransomware targeted a server in the hospital's emergency backup system and later spread via electronic connections to the backup site miles from the main campus and the server farm. The attackers used Microsoft's Remote Desktop Protocol to obtain an entry point into the server and compromised the hardware vendor's administrative account to initiate the ransomware attack. The hackers permanently corrupted the backup files from the systems apart from the digital medical record backup files and demanded four Bitcoins (US$55,000) as a ransom. (4) WannaCry is the most devastating ransomware attack that infected several hospital facilities and services globally. In May 2017, the National Health Services of Britain lost US$92 million in damage due to WannaCry ransomware, which affected patient care [56][57]. (5) Cybercriminals also spread new coronavirus ransomware, which can be uploaded via system optimization software called the fake Wise Cleaner website. People are persuaded to download fake files from the Wise Cleaner website. Upon successfully installing the malware on their mobile devices, their passwords are stolen, and their devices, systems, and the data inside them are encrypted. There is also new ransomware that stops healthcare professionals, patients, and caregivers from accessing the information they have on their devices, infrastructure or network, and cybercriminals demand a ransom in exchange for their release [34][52].

5.2.3 Phishing attacks

Healthcare systems are highly vulnerable and a target of cyberattacks such as phishing because of the value of healthcare information. Javaid et al. [43] defined phishing attacks as social engineering techniques in which adversaries camouflage as legitimate entities and call or send fake e-mails or messages to trick/deceive users to reveal sensitive personal information such as usernames and passwords, credit card details, social security numbers, and health insurance identification numbers that adversaries may use against them. The attackers can use several phishing methods, such as e-mail phishing, spear phishing, vishing, whaling, HTTP phishing, smishing, domain spoofing, malicious websites, and social media phishing, to obtain information about their victims [55]. Phishing attacks are common in the healthcare domain because attackers impersonate legitimate staff or try to gain access to SHSs by calling or sending messages or e-mails or providing a fake link that the staff and patients of the clinic or hospital can use to update their login credentials and fill their sensitive health information. The attackers can then quickly use the entered login credentials to take over the accounts, steal confidential information, harm the system or deploy malware that can block the hospital's server [43][58]. The stolen patient medical records are sold on the dark web or black market. For example, in 2017, attackers used spear phishing to breach the data of New York's largest healthcare provider, Kaleida Health, which compromised over 3000 patients' records.

5.2.4 Eavesdropping attacks

In SHSs, eavesdropping attacks pose a significant threat to violating patients' privacy and healthcare data. According to Chaudhary et al. [53] and Ahad et al. [59], an eavesdropping attack in SHS is where hackers insert themselves on an insecure network path, intercept, modify, delete, and listen to communication between wearable medical devices, biomedical sensors, systems, Wi-Fi, ZigBee or between medical professionals and patients to extract confidential healthcare information such as medical history, medical test results, treatment plans, and payment instrument details for future analysis and performing malicious activities, which may result in privacy breaches [27]. Eavesdropping attacks are also known as sniffing or snooping attacks, and attackers then analyze the intercepted data using software sniffers such as Wireshark [53][60]. Eavesdropping attacks in SHSs are either passive or active [61][62].

5.2.5 Man-in-the-middle attacks

The integrity and confidentiality of healthcare data are jeopardized in SHSs due to severe man-in-the-middle (MiTM) attacks. In the healthcare industry, Haque et al. [63] and Jaime et al. [35] define a man-in-the-middle attack as a malicious attack where adversaries take advantage of the weaknesses in the network connection between two legitimate entities by secretly inserting themselves between their network connection, intercepting, stealing, altering, or deleting the communications sent before forwarding them to the destination address, resulting in a breach of healthcare data, unauthorized access and modification of sensitive healthcare information that can be sold in the black market and used for committing cybercrimes. In SHSs, attackers can intercept medical records from wearable and implantable medical devices, smart devices, biomedical sensors, remote monitoring stations, and databases or that are shared between authentic

healthcare providers by gaining access to a patient's medical history needed for patient care, diagnosis, and treatment [35][61]. Attackers can also use fake base stations to capture and alter information transmitted between smart devices and authentic base stations, compromising smart healthcare data integrity [59][64]. With the MiTM attack, adversaries can change traffic flow, reconfigure the smart healthcare network topology, create phoney identities, and generate malicious and forgery information to compromise the SHS [65]. Sybil attacks, wormhole attacks, identity replication attacks, eavesdropping, and node replication attacks are the different variants of MiTM attacks [65].

5.2.6 Insider threats

Insiders in SHSs constitute a significant security risk since they have legitimate access to patients' healthcare data, systems, and system security. According to Šendelj and Ognjanović [66] and Alsowail and Al-Shehari [67], insider threats are malicious acts perpetrated by authorized persons, such as employees, former employees, contractors, or business partners, who have privileged access to the organization's sensitive information, security practices, network and computer system misuse them to intentionally or unintentionally compromise the confidentiality, integrity, or availability of the organization's digital and physical assets. Insider threats are grouped as malicious, negligent, compromised, disgruntled employees, or third-party insiders and are dangerous because they are not subjected to security procedures [43]. There has been a massive increase in successful insider attacks in healthcare because of carelessness in data sharing, lack of data monitoring, full access privilege to sensitive data, and lack of security awareness, with detrimental effects worse than outside attacks [54]. The insiders within the SHS can access confidential patients' healthcare data, make copies, and sell it to third parties on the dark web for financial gain [8][66]. For example, in November 2020, an employee of the Oregon Lab in Portland Stole 8,000 provided health information, such as names, dates of birth, medical record numbers, provider names, health insurance information, diagnosis and treatment information, and social security numbers, by copying it to a personal storage device without approval.

5.2.7 Medical identity theft

Medical identity theft is the most rapidly rising cyber threat in smart healthcare, accounting for many electronic healthcare fraud cases globally with adverse consequences. Almalawi et al. [52] define medical identity theft as the unauthorized act of cybercriminals using their victims' identifiable confidential information such as their name, date of birth, social security number, health insurance details, and bank and credit card information without consent to obtain or bill for medical services or goods to medicare and other health insurers without the victims detecting until they are billed or receiving incorrect medical treatment. The attackers use the unsecured communication or potential vulnerabilities in the SHS to create fake identifications and steal patients' and healthcare professionals' identifiable information stored and transmitted electronically between healthcare providers, insurance companies, and other entities to obtain healthcare services and bills for medical services, resulting in unforeseen consequences and extensive medical card theft [52]. The adversaries can (1) bill fraudulent medical claims with stolen patient and healthcare professional identities and (2) use healthcare provider medical identifiers to indicate that a physician provided and billed services directly. Meng et al. [68] conducted a survey in the United States and reported that annually, the economic losses due to medical identity theft are close to US$41.3 billion, and over 78% of respondents are worried about the leakage and misuse of personal medical information.

5.2.8 Fake base station

With the cheaper deployment of mobile networks for SHSs, there has been an increase in fake or rogue base stations by cybercriminals, jeopardizing patient privacy and exposing sensitive healthcare data. Liu et al. [64] and Park et al. [69] defined fake or rogue base stations as the use of a software-defined radio to create fraudulent cell phone towers that impersonate the functionality of authentic base stations in a wireless network by tricking users within a certain radius to connect to them. Base stations are vital in wireless communication systems connecting mobile devices and the core network infrastructure. Smart healthcare relies on wireless communication for data transmission between wearable and implantable devices, biomedical sensors, smart devices, and users to implement base stations. Installing a fake base station near smart healthcare will help cyber criminals intercept and alter healthcare information sent between medical devices and legitimate base stations and trick patients and healthcare professionals into connections to unauthentic healthcare services to interfere with the confidentiality, integrity, and availability of smart healthcare data and services. This is achieved by trailing and gathering international mobile subscriber identity data from patients' and healthcare professionals' mobile devices [59][64][69]. Adversaries can use compromised access control and authentication mechanisms to gain unauthorized access to SHSs through fake base stations [64].

5.2.9 Advanced persistent threat

Advanced and well-financed adversaries use several advanced techniques to address persistent threats in smart healthcare to steal sensitive healthcare data frequently and silently. Genge et al. [70] and Khalid et al. [71] defined advanced persistent

threat (APT) as a malicious, sophisticated, and targeted cyber-attack where well-organized and skilled adversaries use several attack tools and techniques to gain illegal access to a network and remain unnoticed for an extended period while steadily and uninterruptedly extracting confidential data, sabotaging the targeted organizational infrastructures or surveillance systems. Advanced persistent threats are caused by adversaries with enough resources and skills to penetrate networks without detection over a long period [72]. Since smart healthcare implements IoMT devices, APT attackers can exploit the weaknesses in smart devices, software, or network infrastructure to illegally gain access to steal sensitive patient healthcare information and compromise the integrity of medical data or medical devices, which can threaten the lives of patients [73]. Before attackers launch APTs, social engineering techniques such as spear phishing, watering holes, SQL injection, and application repackaging are used for collecting the required data about the target, and a successful APT attack typically lasts for a long time [74]. Advanced persistent threats are difficult to detect and prevent since human behavioral variables leading to threats are not considered, there is no evident attack fingerprint, and adversaries conceal their identity while taking advantage of the weaknesses in the compromised system [70][74][75]. Advanced persistent threats pose significant risks in smart healthcare because of the integration of several components, such as wearable and implanted devices, biomedical sensors, medical devices, smart devices, electronic health records, and other interconnected systems, that are used to enhance patient care and operational efficiency. The threats take advantage of the weaknesses in smart healthcare network infrastructure, software solutions, or human error to illegally access sensitive patient medical data, interrupt healthcare services, and manipulate medical devices [72].

5.2.10 Side-channel attacks

Smart healthcare systems consist of several technologies, such as wearable and implantable devices, biomedical sensors, backend servers, and smart devices, that collect and share patient healthcare data using communication channels. These physical devices may include flaws that adversaries might exploit through side-channel attacks to sensitive healthcare information, such as cryptographic keys and passwords. Muhammad et al. [76] and Niksirat et al. [27] defined side-channel attacks in smart healthcare as security threats in which adversaries exploit unplanned information leakage from various channels and computing devices by analyzing physical parameters during their regular operation to collect sensitive healthcare information, such as cryptographic keys and passwords, and send it to a third party. In side-channel and secret attacks, attackers assume that data constantly leak from communication channels such as power consumption, electromagnetic radiation, and timing analysis, which they must exploit [27][77]. This attack is often executed using artificial intelligence techniques, which can identify trends and link sensory data with user activities. Because of their noninvasive nature, they are challenging to manage and pose severe threats [72][78]. Side-channel attacks can be active or passive. Active side-channel attacks require physical access or closeness to the targeted device/system, whereas passive side-channel attacks are silently exploited and undetectable by victims throughout the attack [77]. The three primary side-channel attacks on healthcare systems are electromagnetic, sensor spoofing, and differential power analysis [79], compromising the confidentiality, integrity, and availability of sensitive healthcare data.

5.2.11 Cross-site scripting attack

Cross-site scripting is the most prevalent and vulnerable attack used by adversaries to sneak malicious scripts into websites to steal sensitive user details stored in cookies and web applications, which can result in security breaches. Chaudjary et al. [80] and Sethi et al. [81] define a cross-site scripting attack in smart healthcare as a cyber threat where attackers identify loopholes in the codes of web pages or trusted websites provided by a web server accessed by healthcare users and exploit it by injecting and executing a malicious script to bypass access control, obtain the patients' cookies, steal patient data, hijack sessions, and install malware. The injected malicious script is executed when healthcare users visit compromised web pages or trusted websites, and the attacker can access the patient's healthcare data by impersonating the webcam, microphone, and geographical location [53][82]. The adversaries exploit the flaws in the web applications developed using programming languages like PHP, Java, JavaScript, VBScript, ActiveX, Flash, CSS, and ASP.NET. Web applications built using JavaScript are the most commonly used to build malicious vectors for cross-site scripting attacks [83]. Cybercriminals use cross-site scripting attacks with other attacks, such as cookie theft, phishing, keylogging, identity theft, hacking, DDoS attacks, and cross-site request forgery [83][84]. Cross-site scripting attacks are in different forms, such as stored, reflected, persistent, nonpersistent, and document object model-based [83]. The main objective of cross-site scripting attacks is to execute malicious injected codes into the victim's legitimate web pages or trusted websites to steal users' identities [83]. For instance, adversaries can exploit weaknesses in the web-based interfaces of medical devices, electronic health records systems, patient portals, or other healthcare applications to inject malicious scripts that can give them access to the systems, steal and manipulate sensitive patient information and medical data stored in the SHS, and redirect users to phishing websites to steal login details and trigger actions on medical devices connected to the smart healthcare network that can harm patients.

5.2.12 Session hijacking attack

Internet of Medical Things devices are vulnerable to session hijacking attacks since they rely on unsecured wireless or internet transmission, and the devices retain session connectivity to web application interfaces, where session data can be hijacked. According to Elhoseny et al. [85] and Malhotra et al. [86], session hijacking in smart healthcare is a security attack in which adversaries hijack, modify or redirect the permissible web application session ID of the patient, healthcare professional or web server to gain access to their sensitive healthcare and login credential data during an online communication while the session is still active. Session hijacking attacks, also known as TCP session hijacking attacks, occur when a session is active, and cybercriminals seize the active and legitimate session of the patient/doctor to access the healthcare information being exchanged and participate in the conversation [53]. This is accomplished by deploying a session sniffer, which includes a packet sniffer for altering, seizing, and reading network traffic between the patient/doctor and the web server, as well as the valid session ID, which is created on the client side and stored in the cookies [87][88]. The attackers can also use other techniques, such as cross-site scripting, session fixation, MiTM attacks, and session side jacking, to hijack a user's session. Once the adversary successfully gains access to the session, they can perform actions such as accessing sensitive healthcare data and changing patients' account settings on behalf of the user. Cybercriminals conduct session hijacking to gain unauthorized access to communication between patients, healthcare professionals, and insurance companies [89]. For example, the adversary can steal the session ID or cookie from the patients' or healthcare professionals' web browsers to impersonate and access their accounts and healthcare data or change their session data to inject malicious scripts into the web server or device. Session hijacking compromises the confidentiality and integrity of sensitive patient data.

5.2.13 Zero-day vulnerabilities

Cybercriminals exploit weaknesses in IoMT devices when the firmware is not frequently updated, exposing healthcare users' devices to zero-day attacks since attackers may easily hack and steal sensitive patient medical data [85]. According to Capuano et al. [90] and Patel et al. [91], zero-day vulnerabilities in smart healthcare are security weaknesses in healthcare software, hardware, firmware, or systems that are unknown to healthcare service providers but are exploited by cybercriminals and for which no patch has been publicly released. The method that adversaries use to exploit healthcare software or system vulnerabilities is a zero-day exploit. Zero-day refers to the number of days a healthcare software vendor has known about vulnerability and has zero days to fix or patch the defect [90]. These vulnerabilities allow cybercriminals to compromise the server and gain unauthorized access to sensitive patient medical data, manipulate medical devices that can injure or kill patients without being detected, or disrupt healthcare services, but they are difficult to detect [92][93]. According to the US Cybersecurity and Infrastructure Security Agency, Armis researchers uncovered weaknesses in a pneumatic tube system used by more than 3,000 hospitals globally. The translogic nexus control panel has nine serious flaws that affect all current variants of Translogic's pneumatic tube system (PTS) stations manufactured by Swisslog Healthcare. Pneumatic tube systems are crucial in patient care because they transport drugs, blood products, and laboratory samples across numerous departments. The uncovered vulnerabilities allow an unverified adversary to take over PTS stations and obtain complete control of a target hospital's tube network. The system's vulnerabilities, "PwnedPiper", may be used to gain unauthorized access to a hospital's network and take over Nexus control panel stations [94].

5.2.14 Cryptographic attacks

Healthcare information in SHS is secured using cryptographic techniques to guarantee patient data confidentiality, integrity, and authenticity and to safeguard communication channels between medical devices, servers, and databases. Most of the encryption methods implemented by the developers in these systems are weak, making it easy for cybercriminals to exploit and carry out cryptographic attacks. According to Wasserman and Wasserman [95], a cryptographic attack in smart healthcare is any attempt by hackers to exploit flaws in cryptographic protocols or systems that encrypt sensitive healthcare data or communication to survey, steal, alter, wipe, or damage healthcare records. These systems may have severe problems, such as poor authentication mechanisms and few transactions [96]. The prevalent cryptographic attacks in smart healthcare include brute force, cypher text-only, known-plaintext, chosen-plaintext, MiTM, and side-channel attacks. When developers poorly implement encryption on SHS, it exposes healthcare information stored in the system to eavesdropping, compromising patients' privacy [64].

5.2.15 Stolen physical smart device attack

The popularity of physical smart devices in SHSs has led to increased equipment theft, and the situation is exacerbated when the medical files stored on them are in plaintext. A stolen physical smart device attack is a security threat where adversaries can steal or compromise the physical smart devices used in SHS. Smart devices are implanted and worn by patients or attached to healthcare equipment to collect healthcare data [97]. These devices can be lost or stolen by attackers

who may decide to re-program and redeploy them to access the smart healthcare network and extract sensitive patient data undetected [92][97][98].

5.2.16 Cloud-based threats

Most smart healthcare providers are migrating to the cloud due to the simplicity of retrieving data, the power to store and manage massive amounts of sensitive healthcare data, the ability to analyze medical images, and capability to provide patients with more personalized digital experiences. However, healthcare providers are concerned about cloud security threats since cloud security is available to users anywhere and at any time [43]. Cloud-based threats in smart healthcare are cybersecurity risks that jeopardize the confidentiality, integrity, and availability of sensitive patient data by attacking cloud computing infrastructure and healthcare services. Adversaries exploit the weaknesses in cloud-based platforms and data storage to compromise patient data, disrupt healthcare services, and potentially cause harm to patients. The prevalent cloud-based threats include data breaches, malware and ransomware, insider threats, phishing, DoS attacks, misconfiguration, insecure application programming interfaces, data interception, and compliance and regulatory risks. These threats can hinder patient treatment on a large and life-threatening scale with severe consequences. According to the Netwrix Cloud Data Security report for 2022, cloud breaches are prevalent in healthcare, with 61% of respondents reporting assaults on cloud infrastructure through phishing, ransomware, or other malware attacks.

5.2.17 Medical IoT device vulnerabilities

Medical IoT devices integrate sensors and actuators into SHSs, providing multiple benefits to healthcare professionals and patients regarding efficiency, convenience, and enhanced patient care. However, these devices are prone to critical susceptibilities that cyber criminals may exploit, posing significant risks to patient privacy, security, and safety [91]. Medical IoT devices such as infusion and insulin pumps, smart pens, implantable cardiac devices, wireless vital monitors, medicine dispensers, medical imaging systems, smart thermometers, medical device gateways, biosensors integrated into wearables, temperature sensors, and security cameras have proven to be prone to cyber-attacks because of a lack of built-in controls. These devices are vulnerable to security and data privacy issues, inadequate authentication and authorization, insecure network connections, firmware and software vulnerabilities, DoS attacks, reverse engineering, Sybil attacks using hijacked IoMT, remote brute-force attacks, MiTM attacks, password sniffing, data and key tampering, side-channel attacks, traffic analysis attacks, masquerading attacks, spoofing, radio frequency jamming, malware attacks, data integrity concerns, integration and interoperability challenges, medical IoT device hacking, medical IoT supply chain risks, social engineering attacks, physical security risks, restrictions in power and processing capabilities and scalability, and biocompatibility [99][100]. These attacks can result in the inaccessibility of SHS resources, physical injury to ambulance- or hospital-bound patients, and adversaries gaining unauthorized access to the smart healthcare network [93]. According to a recent Cynerio healthcare cybersecurity survey, 56% of hospitals have targeted their IoMT equipment, with 88% of data breaches involving IoT devices and 53% of medical IoT devices having at least one major vulnerability [101].

5.2.18 Attacks associated with blockchain

Blockchain technology is gaining significant attention in smart healthcare because of its potential to improve user anonymity, data privacy, integrity, transparency, nonrepudiation, decentralization, traceability, immutability, confidentiality, interoperability, traceability, and success in exchanging healthcare data [102][103]. However, blockchain in smart healthcare is also vulnerable to attacks, which can threaten the security of healthcare data stored in SHSs, thus impeding their integrity, confidentiality, and availability. Blockchain technology has introduced new cybersecurity threats in SHSs, including routing attacks, private key security attacks, high bandwidth consumption, throughput problems, poor scalability, MiTM attacks, eclipse attacks, Sybil attacks, decentralized autonomous organization attacks, Parity Multisig Wallet attacks, Finney attacks, race attacks, Timejack attacks, mining malware, selfish mining attacks, 51% attacks, double spending, smart contract vulnerabilities, DoS and DDoS attacks, privacy attacks, blockchain forks and consensus issues, and hacking, which gives the adversaries with the chance to access medical records stored in SHSs illegally [104].

5.2.19 Poisoning attacks

In poisoning attacks, adversaries alter the SHS's training data and introduce malicious samples to confuse the machine learning/deep learning model's learning process, causing retraining efforts to fail [29]. The attackers are aware of the machine learning model's healthcare data distribution and modify the value of the input data via data injection, modification, and logic corruption methods to a certain extent. This impacts the entire learning process of the SHS machine learning model by misdiagnosing test results, which may result in patient maltreatment. Poisoning attacks are challenging to detect and can result in incorrect diagnoses by computer-aided diagnostic systems, delaying and compromising treatment, jeopardizing healthcare data integrity and patient monitoring systems, posing security risks in telemedicine, manipulating

drug discovery and development, and undermining trust in artificial intelligence systems [45]. A hypothyroid diagnosis may have life-threatening effects, whereas a false-positive COVID-19 classification may induce undue fear [45].

5.2.20 Model stealing/inversion

Model stealing, also known as model inversion, occurs when attackers analyze a black-box machine learning/deep learning system to recreate a confidential model or obtain sensitive training data or training data attributes. The attackers also acquire data by querying a victim model and training a substitute model to steal the target model's functionality [29]. In 2020, cybercriminals successfully cloned the convolutional neural network model for predicting lung cancer complicated by pulmonary embolism using only a small amount of labeled data from the target convolutional neural network. This poses significant threats to computer-aided diagnostic systems trained with machine learning/deep learning models and patients' private data [45]. Model stealing/inversion impacts various healthcare artificial intelligence applications by breaching privacy, having ethical concerns, posing security problems, and causing prejudice and discrimination.

5.2.21 Legacy systems

Healthcare providers depend on legacy systems that lack up-to-date security features for delivering healthcare services, thus exposing them to potential cyberattacks. Pandagle [105] defined legacy systems in smart healthcare as outdated hardware (e.g., servers, networking equipment, medical equipment), software (e.g., operating systems and other applications), and network infrastructure developed using obsolete programming languages that the manufacturer no longer supports because of incompatibility with modern technologies or standards. Smart healthcare systems store massive amounts of sensitive healthcare data, and many providers rely on outdated systems to share healthcare resources internally. Using such systems to share medical data with different healthcare institutions is challenging [106][107]. Adversaries consistently target and exploit such systems, exposing critical healthcare data to possible assaults due to a lack of security updates [95][105][108]. For example, in January 2018, the Southeast Norway Regional Health Authority announced that attackers had compromised 2.9 million patient health records by exploiting flaws in the Windows XP legacy system.

5.2.22 Regulatory compliance challenges

To be fully regulated, healthcare providers must comply with strict regulatory and compliance requirements, as outlined in the HIPAA and GDPR. Different regions have specific rules and standards for handling, storing, and transmitting patient healthcare data globally. Patients have control over their data and can only give it to third parties based on their consent, except if otherwise stated in the regulatory requirements [109]. Besides, the HIPAA explicitly states that the regulations and standards for IoMT devices must follow so that healthcare institutions implementing SHSs may apply suitable security procedures to protect patients' healthcare data. However, some healthcare providers do not comply with the regulations, thus compromising patient healthcare data and resulting in severe penalties. In smart healthcare, regulatory compliance challenges are the hindrances and difficulties that regulatory bodies, healthcare providers, and technology developers face to guarantee compliance, healthcare data security, patient and healthcare provider privacy, and healthcare safety standards within fast-growing healthcare technology. In the healthcare industry, most wearable medical devices that support general wellness are grouped in Class I because they do not meet the current medical device standards; other devices meant for medical reasons are grouped in Class II and III, which need strict certification procedures and regulatory approvals; and the International Electrotechnical Commission 62304 reference standard for medical software only describes the software lifecycle. These defects have become a major challenge for software engineers developing intelligent health homes [110]. The regulatory compliance of smart healthcare providers faces several challenges because of healthcare data confidentiality and the multifaceted regulatory landscape of the healthcare sector. Regulatory compliance challenges include (1) a lack of healthcare data standards, (2) regulatory uncertainty, (3) the scarcity of technical expertise among regulatory staff, (4) interoperability standards issues, (5) a shortage of patient control, (6) regulatory variations, (7) cybersecurity talent shortage systems, (8) data ownership issues, (9) compliance with data protection laws, (10) repeated monitoring and adaptation, (11) cybersecurity risks, (12) emerging technology regulation, (13) the trailing and management of standards and regulations, (14) technical, legal, and regulatory barriers, (15) the interpretation and understanding of regulations and standards, (16) ever-changing regulations, (17) compliance training challenges, and (18) a lack of agreement [25][111][112].

5.3 Integrity Attacks

The existing threats to integrity include the following:

5.3.1 Tampering attack

Cybercriminals in the healthcare sector can tamper with medical wearable, implantable, biomedical sensors and smart devices by exploiting the weaknesses in their firmware and installing malware that can give them access to sensitive patient healthcare data. According to Chaudjary et al. [80] and Lin et al. [113], a tampering attack occurs when adversaries illegally

alter or manipulate medical devices or systems connected to a healthcare network to modify SHS data, user credentials, patient medical history, and location, as well as disrupt communication between IoMT devices and servers or implant malware to disrupt IoMT device functionality. The attackers use the MiTM attack to access data from the IoMT devices and distort the medical records [80]. The main aim of tampering attacks is to compromise the integrity of healthcare data exchanged between IoMT devices and healthcare providers, possibly resulting in incorrect diagnoses and decision-making [73]. Examples of tampering attacks in smart healthcare include (1) hackers tampering with the data collected using medical devices, resulting in misdiagnosis or incorrect treatment; (2) cybercriminals gaining unauthorized access to medical devices or systems, thus interfering with their functionality, patient treatment plans or stealing sensitive patient information; and (3) adversaries using ransomware to encrypt patient data in medical devices or systems and disrupt healthcare services until a ransom is paid for the release of a decryption key.

5.3.2 Cookie manipulation attack

According to Chaudjary et al. [80], a cookie manipulation attack is a cyber-attack in which cybercriminals exploit vulnerabilities in cookies within a healthcare system's web application to obtain and steal patients' identities and sensitive information by manipulating and forging the cookies. A cookie is a small text file that stores data about the websites the user visits in the user's browser and device. Attackers can easily intercept, modify, or forge their content if such a text file is not secured because it contains sensitive information about patient ID, usernames and passwords, medical records, and other personal information. They can use compromised sensitive data to gain unauthorized access to patients' accounts and perform other malicious actions, such as impersonating genuine users, retrieving patient records, interfering with medical information, or compromising the integrity of the SHS [53][80]. For example, when patients and healthcare professionals log into SHSs, their username, password, and other medical or personal data are stored in cookies. Cybercriminals can illegally access these cookies, manipulate their stored data, and steal their login credentials and health insurance identification numbers.

5.3.3 Supply chain attacks

Most healthcare providers globally rely on third-party vendors to develop and implement SHSs. These third-party vendors have weaknesses in their systems, creating a potential weakness in their security system that cybercriminals can exploit by introducing malware to attack healthcare providers' SHSs through software updates. In smart healthcare, a supply chain attack is a cyber-attack in which adversaries target and exploit medical devices, software systems, communication networks, and other components of healthcare infrastructure and supplier networks with healthcare service providers to overcome system flaws [102]. Healthcare providers work with several third-party vendors and can introduce possible cybersecurity risks when they have insecure systems and practices. The attackers take advantage of the susceptibilities in the supply chain to illegally gain access to sensitive healthcare information, disrupt healthcare services, or compromise the integrity of healthcare data. The Ponemon Institute conducted a poll and discovered that 63% of healthcare IT professionals believe that their firms are susceptible to supply chain attacks, with 40% expressing fear [114]. For example, adversaries can hack the software used to operate insulin pumps or pacemakers by inserting malicious codes into devices where they can control them, putting patient health at risk.

5.3.4 Medjacking

Medjacking is a new type of cyber-attack in which adversaries remotely target internet-connected SHSs and medical devices with high-value patient healthcare data. Wilner et al. [115] and Kirubakaran et al. [116] define medjacking as the practice where hackers use malware to attack and manipulate medical devices and instruments and healthcare systems and networks to create backdoors to breach their security and harm patients. Once attackers successfully create a back door, they can illegally access, manipulate, and control software of medical sensors, steal sensitive patient healthcare data from insulin pumps, diagnostic equipment, pacemakers, monitoring devices, infusion pumps, defibrillators, and other network-connected medical devices; or launch a ransomware attack [115][116]. Examples of medjacking include (1) according to TrapX, cybercriminals used malware to infect several medical machines (e.g., radiation oncology system, trilogy LINAC gating system, and fluoroscopy radiology system), medical devices (e.g., surgical blood gas analyzers) in a hospital and used the equipment as a backdoor for accessing passwords from the hospital's IT system and sensitive healthcare data; and (2) hackers also identified the serial numbers of the IoT medical devices such as a pacemaker or insulin pump and manipulated the functionality of the devices, thus threatening the physical health of the individuals. Hackers can easily hack the delivery pump and misuse it by injecting an abnormal insulin dosage into the human body, which can cause severe and life-threatening consequences [115].

5.3.5 SQL injection attacks

Many SHSs are web-based and store healthcare data in SQL databases, making them susceptible to SQL injection (SQLi) attacks. Noman and Abu-Sharkh [117] and Abdullayev and Chauhan [118] define SQLi attacks as a type of application security susceptibility in which cybercriminals exploit SQL database weaknesses by injecting malicious SQL codes/statements into the input fields of a website and desktop and mobile application forms or URL parameters to compromise the back-end database and illegally access and extract sensitive data stored in the database. Numerous websites implement SQL to manage their database, and attackers take advantage of the weaknesses in SQL to execute malicious SQL statements, which allows the servers to reveal sensitive information stored in the databases. To carry out SQLi attacks, adversaries target website input fields and desktop and mobile application forms that have not been appropriately validated [117][118]. In smart healthcare, patients and healthcare professionals use smart healthcare software to access data that can be shared with other departments. If the forms are not correctly validated, attackers can insert malicious SQL statements into the forms filled out by patients and healthcare professionals. A successful SQLi attack can extract sensitive patient healthcare data stored in the underlying database, affecting the system's confidentiality, integrity, and availability [53][73][119]. For example, (1) in May 2016, hackers used SQLi to attack 33 Turkish hospital databases where more than 10 million medical healthcare records were leaked; (2) in early 2016, hackers also compromised the personally identifiable information of 1400 employees of York Hospital in Maine; and (3) in 2015, it was discovered that Epiphany Cardio Server version 3.3, a central web application used for managing hospital data, had vulnerabilities that could allow the execution of SQL injections.

5.3.6 Buffer overflow

Buffer overflow attacks have devastating effects on the cybersecurity of SHSs. According to Veluvarthi et al. [120], a buffer overflow in smart healthcare is a security vulnerability in which adversaries exploit weaknesses in the SHS or system by sending excessive patient data to the buffer, resulting in a system crash, malicious code execution, or unauthorized access. When excess data are put into the buffer, some extra information can leak or spill into other adjacent memory locations, thus corrupting or overwriting the information they store, causing the program to crash or execute random code [85]. When adversaries take advantage of such vulnerability, they can change the behavior of the SHS, access sensitive patient healthcare information, temper with medical devices or change patient treatment plans. Besides, when the smart healthcare network traffic load increases, it may result in buffer overflow, high data retransmission, and degradation of the quality of service regarding latency, packet loss, throughput, and energy consumption [121][122].

5.3.7 Routing attacks

Adversaries use routing attacks on the internet service providers' side to exploit the weaknesses in the internet infrastructure to change the routing tables. Veluvarthi et al. [120] and Mohammed et al. [104] define routing attacks as a form of cyber-attack where cybercriminals poison and manipulate the routing table or information to redirect traffic/transmit data packets to malicious devices of attackers for interception, manipulation, and blockage of network traffic, causing severe damage to the healthcare network infrastructure. This attack can significantly compromise patient privacy, data confidentiality, integrity, availability, and overall SHS security [53][97]. Routing attacks can take numerous forms, including router, select, forwarding, and replay attacks [123].

5.3.8 Sensor attacks

Wireless sensor networks are commonly employed in SHSs to gather and analyze patient data via wearable, implantable, and biological sensors. These sensors occasionally fail to function or die due to a lack of power, thus allowing hackers to infiltrate the network or replace faulty sensors with compromised ones to carry out malicious acts more effectively [24]. In SHSs, sensor attacks are cybersecurity threats and vulnerabilities targeting biomedical sensors in healthcare devices and systems. When patient data in medical sensors are not adequately protected, cybercriminals can easily compromise them by injecting false data. Attackers can also exploit the weaknesses of real-time location service devices to illegally obtain patient data [73][85].

5.3.9 Evasion attacks

In evasion attacks, attackers attempt to trick the SHS using adversarial samples while testing. The attackers have no impact on the training healthcare data but may get access to the machine learning model and gather adequate information. They attack and manipulate the machine learning model, misclassifying the SHS patient status [29][124]. Evasion attacks attempt to manipulate test data such that the model generates incorrect predictions, interrupts services, or jeopardizes the system's integrity. Data manipulation, identity faking, traffic pattern analysis, protocol exploitation, and encryption cracking are among the most prevalent evasion attempts in smart healthcare. Evasion attacks fall into two categories: white-box attacks and black-box attacks. In white-box attacks, attackers have in-depth knowledge of the machine learning model used in the

training phase and have access to the training data distribution at the SHS. Common white-box attacks in the SHS machine learning model include HopSkipJump, the fast gradient method, Carlini & Wagner, and decision tree-based methods. In black-box attacks, the attackers do not know the SHS machine-learning model but utilize knowledge about settings or previous inputs to assess the model's vulnerabilities. The zeroth-order optimization attack is an example of a black-box attack in the SHS. Machine learning/deep learning algorithms in computer-aided diagnostic systems face challenges because intelligent and adaptive adversaries can carefully manipulate the input medical image data to bypass the detection system's performance and violate the medical image data [45]. Evasion attacks have severe consequences for patient safety, data privacy, and the reliability of healthcare artificial intelligence systems.

5.4 Availability Attacks

The existing cybersecurity threats against availability include the following:

5.4.1 Denial-of-service (DoS) and Distributed DoS (DDoS) attacks

Recently, there has been an increase in DoS and DDoS attacks on SHSs because of the sensitivity of healthcare and financial data [125]. Wasserman and Wasserman [95] and Talati and Chaudhari [61] define a DoS attack in smart healthcare as a form of attack where cybercriminals overwhelm the network of SHSs and servers with fake traffic so that the servers or smart devices cannot respond to the requests of legitimate healthcare professionals and patients either temporarily or permanently. In a DDoS attack, the fake traffic used to flood the network of SHSs and targeted servers comes from distributed endpoints and IoT devices that are recruited by the attackers to be part of the botnets using malware infection, thus making the healthcare services unavailable to the legitimate users [43]. Cybercriminals can use hacked or fake base stations to launch DoS attacks, thus disrupting the network of medical sensors and devices to the authentic SHS network and rendering crucial healthcare services unavailable to patients and healthcare professionals [64]. In a DoS attack, patient healthcare data can also be accessed by third parties without authentication and authorization, giving the attackers privileges to alter the patients' healthcare data and send fake patient information, resulting in false treatment and false emergency calls to caregivers [27]. Distributed DoS attacks are simple to launch by attackers and may result in difficulty accessing patients' healthcare and financial data, treating patients, and preventing their launch [43]. A DDoS attack significantly impacts the availability, capacity, and performance of a smart healthcare network [55]. Adversaries sometimes use DDoS attacks with Ransomware to make patient care difficult since they prevent healthcare professionals from accessing their vital healthcare records. Recent examples of DDoS attacks include (1) those that targeted the Department of Health and Human Services website in the United States. It overwhelmed the server hosting the department's website, disrupting operations and leading to the closure of the fundraising website [34], and (2) the pro-Russian hacktivist group 'KillNet', which attacked US healthcare systems by conducting several DDoS attacks in response to the US backing for Ukraine in the Ukraine-Russia War. The adversaries used this attack to send requests and packets to the target server or website every minute, delaying or disabling susceptible systems for hours or days.

5.4.2 Jamming attacks

With the widespread implementation of wireless sensor networks in smart healthcare, jamming attacks disrupt wireless communications via selective or nonselective jamming assaults. According to Srhir et al. [87], jamming attacks are a type of DoS attack in which adversaries send high-range radio frequencies or use malicious jamming nodes to disrupt or interfere with wireless communication signals used by sensor nodes in medical devices or smart healthcare networks. The adversary uses a jammer device with less energy to randomly generate a radio signal that matches the frequency sent by medical sensor nodes to disrupt other signals transmitted by a medical sensor node from the patients and healthcare providers and receives within the adversary's range so that the nodes within the attacker signal range are inaccessible as the jamming signals continue [53][87]. Jamming attacks have high energy efficiency, low detection chances, and anti-jamming resistance and are classified as constant, intermittent, random, intelligent, deceptive, or reactive jamming attacks [126].

5.5 Authentication Attacks

The existing cyber security threats against authentication include the following:

5.5.1 Impersonation attacks

With the massive amount of valuable healthcare information, SHSs face numerous cybersecurity threats, with impersonation attacks being the most predominant. Sharma and Singh [127] define an impersonation attack in the context of smart healthcare as a type of cyber-attack where an adversary fraudulently disguises a trustworthy user's identity, secret key or device within the healthcare communication system to gain access to the victim's sensitive information or systems or perform malicious activities. Impersonation attacks can be achieved by attackers stealing login credentials, using fake identities, manipulating network traffic, bypassing the authentication mechanism or manipulating security vulnerabilities

to avoid detection [53]. In SHS, attackers can illegally access confidential healthcare data from wearable and implantable devices, biomedical sensors, and medical equipment when there are weaknesses in the system and then spoof healthcare service providers by cracking the traffic analysis and pairing secure PINs [53]. Recently, healthcare providers have developed mobile applications that patients and caregivers can use to access healthcare services. They must download and install such healthcare applications on their smart devices. Attackers are taking advantage of the lack of or slow regulation of online app stores to create fake healthcare mobile applications that resemble genuine healthcare applications for healthcare providers to dupe victims by marketing them in poorly regulated app stores. When the victims download such fraudulent healthcare applications and try to log in with their secure login credentials, their details are submitted to the cybercriminals, who use them to perform healthcare services on behalf of their victims. In addition, cybercriminals can use reverse-engineering methods to sniff the device's PIN in insecure communication between a glucose monitoring device and the insulin delivery system and use such PINs fraudulently to authenticate patients [79].

5.5.2 Brute-force attacks

Hackers utilize brute-force attacks to obtain unauthorized access to SHS by exploiting authentication flaws. In smart healthcare, a brute-force attack is a form of cybersecurity threat where hackers use a trial-and-error method to systematically guess the possible login credentials, usernames and passwords, and encryption keys until they match the correct one to gain unauthorized access to sensitive SHSs, medical information, or devices within a healthcare setting [47]. The attackers launch brute-force attacks to target wearable and implantable devices, biomedical sensors, and smart devices with inadequate security measures to acquire patients' credentials and medical information for fraud [92]. Automated software can be used to churn through countless usernames and password combinations to breach the login credentials of SHSs until they can access the system. They can install malware, steal patient medical records or manipulate medical data once they log in successfully [35]. Jaime et al. [35] reported that cybercriminals penetrate remote patient monitoring biomedical microelectromechanical systems by exploiting password weakness on a connected mobile application. When they gain access, they change the device parameters, thus making it transmit inaccurate vital signs and changing the patient's treatment schedule.

5.5.3 Replay attacks

Smart healthcare systems store vast amounts of sensitive patient data, subjecting them to various security threats and dangers, including replay attacks that are difficult to detect. A replay attack in SHS is a type of cyber-attack where adversaries eavesdrop on the communication between biomedical sensors, smart devices, healthcare providers, or users, capture and record login credentials or patient data, fraudulently delay, and resend the recorded data to deceive the healthcare system or gain unauthorized remote access to sensitive patient medical information and the healthcare system as if it comes from the original sender [128][129]. Attackers carry out replay attacks to build trust in intelligent healthcare networks.

5.5.4 Account hijacking

Many IoMT devices use weak encryption or send data over the internet in plaintext, allowing attackers to capture packets while users authenticate, resulting in hijacking. In SHSs, account hijacking is a cyber threat where adversaries hack healthcare users' accounts to gain unauthorized access and control, compromise, and steal the sensitive healthcare data stored in the SHS or platform to perform malicious actions [130]. For example, cybercriminals can hijack patients' and doctors' accounts and modify, distort, and jeopardize sensitive healthcare data by using weak passwords or social engineering [131]. The rise of account hijacking in smart healthcare is due to unpatched vulnerabilities in IoMT devices and old operating systems [82]. Phishing is the most popular type of account hijacking in the healthcare industry [131].

5.6 Authorization Attacks

The existing cyber security threats against authorization include the following:

5.6.1 Cross-site request forgery attack

The Internet of Medical Things systems and devices that use RESTful application programming interfaces are prone to cross-site request forgery attacks when not correctly configured. In smart healthcare, cross-site request forgery is a web security susceptibility where cybercriminals trick or deceive healthcare users into executing unintended actions on web applications to which the users are fully authenticated or logged in without their consent. Attackers execute cross-site request forgery attacks by exploiting the weaknesses in managing cookies via web applications. Upon a successful user login to the web application and with the help of social engineering, cybercriminals can exploit the user's active session to trick them into executing unwanted actions on the compromised web application without their knowledge [82]. This is possible using common HTML elements and JavaScript, making it simple to execute the attack to illegally collect patient

personal information, change account settings, bypass the authentication mechanism, and commit fraudulent transactions [132]. For example, an adversary can write malicious code and inject it into a legitimate SHS. When a healthcare provider or patient successfully signs into the SHS, it sends a request to the SHS to perform tasks such as manipulating medical records and prescriptions and illegally accessing sensitive healthcare data. Cross-site request forgery attacks are used in conjunction with phishing.

5.7 Trustworthiness Attacks

The existing cyber security threats against trustworthiness include the following:

5.7.1 Sybil attacks

Sybil attacks are the most common and dangerous routing attacks in smart healthcare, targeting wireless sensor networks by forging device identities to steal patient medical information. Hassan et al. [133] and Shaji and Nair [134] define a Sybil attack in smart healthcare as a security threat in which adversaries create multiple fake identities or nodes (Sybil nodes) from a single node in a healthcare network by observing their behavior to gain control or disrupt the communication lines, storage, and operation of an SHS, as well as to affect the overall network performance. A node in the smart healthcare network system provides the victim node with multiple fake identities to perform a single operation multiple times. The victim's node will transmit data through the compromised nodes, thus exposing sensitive patient medical data, misinterpreting the victims in the network, and increasing routing turbulences [85][135]. For instance, (1) the Sybil assailant may create, suspend or transmit incorrect patient data for poor diagnosis, increasing patient safety risks by delivering substandard or no medical treatment [136], and (2) the Sybil node can transmit malware that the attacker can use to conduct a DDoS attack to interfere with legitimate nodes [87]. Sybil attacks can be used with message suppression and channel jamming attacks [45]. The main objective of the Sybil attack is to manipulate the network devices and interrupt the communication process without deploying physical nodes [134][137]. These attacks are categorized as SA-1, SA-2, and SA-3 [134][137].

The potential consequences of cyber threats in smart healthcare can be severe and far-reaching, such as reputational damage to healthcare providers, loss of patient trust in healthcare systems, financial losses to healthcare providers and patients, disruption and denial of medical service, breach of confidential patient information, violation of patient privacy, medical identity theft, loss of access credentials, breach of confidential patient healthcare records, data interception from IoMT devices, misdiagnosis leading to medication overdose, IoMT device tampering, regulatory compliance violations and penalties, intellectual property theft, patient safety risks, delayed treatment and incorrect prescriptions, spread of malware, compromise of device authentication, introduction of fake medical devices, patient physical harm or death, recruitment of botnets, illegal monitoring and disruption of critical network or system infrastructure, supply chain attacks, successful extraction of encryption keys from devices, theft of session cookies, credential phishing, medical fraud and errors, interoperability issues, lack of artificial intelligence transparency and explainability, algorithmic biases, and launch of DoS, MiTM, side-channel, and impersonation attacks [64][69][74][75][87][118][134][136][136][138]. Table II summarizes the potential cyber threats in SHSs based on the security requirements they violate.

TABLE II. SUMMARY OF THE POTENTIAL CYBER THREATS IN THE SMART HEALTHCARE ECOSYSTEMS BASED ON THE SECURITY REQUIREMENTS THEY VIOLATE.

S/No	Security Requirement	Cyber Threat	References
1	Privacy	Privacy concerns	[30][43]
2	Confidentiality	Data breaches	[2][31][37]
		Ransomware	[32][34][43][52]
		Phishing attacks	[43]
		Eavesdropping attacks	[27][59]
		MiTM attacks	[35][64][59]
		Insider threats	[43]
		Medical identity theft	[52]
		Fake base station	[59][64][69]
		Advanced persistent threat	[26][70][71][74][75]
		Side-channel attacks	[76]
		Cross-site scripting attack	[81][82]
		Session hijacking attack	[87][88]
		Zero-day vulnerabilities	[91]
		Cryptographic attacks	[64][83]
		Stolen physical smart device attack	[8]
		Cloud-based threats	[43]
		Medical IoT device vulnerabilities	[91]
		Attacks associated with blockchain	[37][104]

		Poisoning attacks	[29][45]
		Model stealing/inversion	[29][45]
		Legacy systems	[105][107]
		Regulatory compliance challenges	[25][111][112]
3	Integrity	Tampering attack	[113]
		Cookie manipulation attack	[53][80]
		Supply chain attacks	[114]
		Medjacking	[116]
		SQL injection attacks	[117][118]
		Buffer overflow	[120]
		Routing attacks	[104][120]
		Sensor attacks	[24]
		Evasion attacks	[29][45][124]
4	Availability	DoS and DDoS attacks	[27][34][43] [64]
		Jamming attacks	[87]
5	Authentication	Impersonation attacks	[127]
		Brute-force attacks	[35][47]
		Replay attacks	[129]
		Account hijacking	[82][130]
6	Authorization	Cross-site request forgery attack	[82]
7	Trustworthiness	Sybil attacks	[45][87][133][134]

Table II outlines the security principles violated by the various cyber threats in smart healthcare systems. Various privacy concerns violate privacy: confidentiality is violated by data breaches, ransomware, phishing attacks, eavesdropping attacks, MiTM attacks, insider threats, medical identity theft, fake base stations, advanced persistent threats, side-channel attacks, cross-site scripting attacks, session hijacking attacks, zero-day vulnerabilities, cryptographic attacks, stolen physical smart device attacks, cloud-based threats, medical IoT device vulnerabilities, attacks associated with blockchain, poisoning attacks, model stealing/inversion, legacy systems, and regulatory compliance challenges. Tampering, cookie modification, supply chain attacks, medjacking, SQL injection, buffer overflow, routing, sensor, and evasion attacks violate integrity. In contrast, DoS and DDoS attacks, as well as jammer attacks, violate availability. Impersonation attacks, brute-force attacks, replay attacks, and account hijacking violate authentication. Cross-site request forgery attacks compromise authorization, whereas Sybil attacks undermine trustworthiness.

6. SECURITY MECHANISMS IN SHS

With the integration of emerging technologies into SHSs, effective cybersecurity measures are required to secure sensitive patient healthcare information and maintain the smooth operation of healthcare systems. The following security techniques are employed to mitigate cyber threats in SHSs.

6.1 Cryptographic-based techniques

By applying cryptographic principles, smart healthcare systems use cryptographic-based techniques to protect sensitive healthcare data. To protect healthcare data privacy and verify healthcare data authenticity and authority, symmetric-key cryptography, asymmetric-key cryptography, and hash-key cryptography are used in conjunction with a digital signatures and cryptographic primitives such as identity-based encryption, shredicate/hierarchical pantograph encryption, and (fully) homomorphic encryption [139]. The Data Encryption Standard (DES), Triple Data Encryption Standard (Triple DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), Secure Hash Algorithm 2 (SHA-2), SHA-3, Hash-based Message Authentication Code (HMAC), digital certificates, and quantum cryptography are the cryptographic algorithms employed in SHS to encrypt healthcare data at end-to-end, rest, in transit, and during backup processes [35][110][140][141]. Medical data are securely encrypted before being transmitted to the cloud or between storage and transmission [45][142]. To provide safe communication, cryptographic algorithms are used for IoMT devices and sensors. The SHS can use the patient's biometric information captured from electrocardiograms, fingerprints, face, retina, iris, voice, and other biometric data. Biometric cryptography can secure sensitive healthcare data by generating a digital key from a biometric or binding a digital key to a patient's biometric. Cryptographic-based algorithms help ensure healthcare data privacy, integrity, confidentiality, user authentication, nonrepudiation, and attack resistance [143].

6.2 Digital watermarking

Healthcare professionals and radiologists routinely share patients' clinical data and information stored in the SHS via the cloud or the internet to aid in clinical evaluation, patient diagnosis, and research. The shared clinical data can be audio, video, or images and, if not strongly protected, may be subjected to breaches, modifications, snooping, deletions, copying,

illegal access, copyright infringement, misdiagnosis, or even death. Several strategies have been developed to safeguard the exchange of medical images and data. Digital watermarking is the most secure technique for protecting medical images, copyrights, and intellectual property [144-146]. Yan et al. [45] and Gull & Parah [146] define digital watermarking as a technique for embedding or hiding distinct imperceptible digital signals, information, or markings within medical images, video, audio, and other multimedia or documents to provide authentication, integrity verification, and copyright protection. Digital watermarking is required in SHSs to identify healthcare users and secure medical images that carry sensitive patient information [146]. The digital watermark may include the physician's signature, a unique patient number, and diagnostic information [147]. Spatial and frequency domain-based approaches embed data into an image [147], whereas medical image authentication employs image-based and self-generated watermark embedding [147]. Digital watermarking techniques protect medical images such as X-rays, magnetic resonance imaging, computed tomography scans, ultrasound images, and metadata within research documents, datasets, and publications by concealing information about the patient, imaging facility, and acquisition parameters. They also protect medical video streams and teleconsultation sessions by hiding timestamps, session identifiers, and encryption keys in video feeds that are difficult to access and manipulate [45][146]. Medical data protected by a digital watermark can then be sent to healthcare providers in the smart healthcare network. After obtaining the medical data, healthcare users can compare it to the extracted unique digital watermarks and parameters to ensure its validity and integrity [45]. Medical image watermarking techniques have a variety of applications, including authentication and integrity verification, medical prescriptions, sensitive patient data protection, medical image authentication, medical image clinical trials and research, and medical image medical video and telemedicine [147]. Digital watermarking is used in SHSs to protect the security and trustworthiness of digital medical data, as well as to verify the integrity, confidentiality, and authenticity of medical images [45][142][147][148].

6.3 Digital steganography

The exchange of medical information between healthcare experts and providers in SHSs has made patient privacy a top consideration. Protecting medical information, especially medical images such as X-rays, radiography, ultrasound, magnetic resonance imaging, and positron-emission tomography, is critical since they aid in diagnosis and can save a patient's life. Encrypting the patient's medical information and images attracts adversaries, but this problem may be solved by utilizing digital steganography to hide the patient's medical information in a public cover image [149]. According to Yan et al. [45], digital steganography in smart healthcare is the technique of imperceptibly concealing sensitive medical data within other medical images (cover medium) to ensure confidential and trustworthy communication while restricting access to such sensitive medical data. Protecting sensitive patient data and other health records with digital steganography is essential since they are accessible only to physicians and other healthcare workers upon request [45]. Digital steganography embeds patient medical information, such as patient records, diagnostic images, or treatment plans, into apparently harmless digital files such as text, images, audio, or video streams to secure patient data within diagnostic images and improve the security of smart healthcare platforms, preventing unauthorized access to sensitive medical information. Embedding the patient's medical information into the cover medium produces stego, which may be communicated to the recipient. Digital steganography techniques use cryptography to encrypt patient medical information and embed it into the cover medium to provide further protection. The message, carrier, and stego-key are all components of digital steganography. The message is that sensitive patient medical information in text, picture, video, or audio is protected using steganography. The carrier is how the key and cover media are communicated. The stego-key is the password for protecting sensitive patient medical information [150]. The main goal of digital steganography in smart healthcare is to conceal confidential patient information in digital media (such as movies, audio, and images) without causing numerous changes in the actual image, and security is improved by combining the steganography mechanism with a cryptographic mechanism, making it more difficult for unauthorized parties to discover or access sensitive patient information [45][150]. Digital steganography techniques are grouped into spatial domains (least significant bit, most significant bit, and other spatial hiding) and frequency domains (discrete cosine transform and discrete wavelet transform) based on their embedding domains [150]. Privacy preservation, data integrity, secure communication, medical imaging, telemedicine, and authentication are potential uses of digital steganography in smart healthcare. Digital steganography in smart healthcare protects patient privacy by hiding sensitive medical data within nonsensitive files to prevent unauthorized people from accessing and interpreting hidden information; it also facilitates secure communication between healthcare professionals by embedding patient data within communication channels; it improves the confidentiality and robustness integrity of stenographic transactions in smart healthcare; and it resists cyber-attacks [150].

6.4 Pseudonymization-based techniques

Smart healthcare systems use pseudonymization-based strategies to protect patient privacy by linking them with datasets only under specified and regulated conditions. According to Louassef and Chikouche [151], pseudonymization is a technique in which a patient's identity data are removed and replaced with cryptographically generated tokens or specifiers

(pseudonyms) that cannot be linked to his or her identification data unless a secret is known. Pseudonyms are secret random numbers that link patients to their medical data stored in SHS and replace their identity before sharing the medical data. They can only be recovered after authorization, making it impossible for attackers to connect the patient's medical data to the pseudonym. Therefore, pseudonymization is a patient-controlled, reversible process under certain conditions. A pseudonymized healthcare database must have two tables: one for permanently keeping all patient medical and personal information and another for storing pseudonyms and pseudonymized data. Tokenization, data masking, hashing, randomization, selective disclosure, and dynamic pseudonymization are examples of pseudonymization-based techniques used in SHS. Pseudonymization-based strategies are applied in identity management and e-prescriptions. The potential benefits of pseudonymization-based techniques in SHSs include healthcare users trusting SHSs because their identities are hidden, ensuring healthcare data privacy and security and preventing adversaries from accessing sensitive patients' healthcare data [151][152].

6.5 Digital signature

IoMT devices create massive volumes of patient medical data that are kept in smart healthcare databases. These patients' medical data are confidential because other parties can interfere with it, endangering the patient's life, causing injury, or selling it on the dark web. Creating a digital signature authentication mechanism for smart healthcare can assist in solving this problem. Jamroz et al. [153], Rani et al. [154], and Ahmed et al. [139] described digital signatures as a cryptographic mechanism for protecting IoMT devices and SHSs, as well as for authenticating and authorizing legitimate healthcare users to access and utilize sensitive medical data held in healthcare systems. In SHSs, healthcare professionals, patients, and other authorized parties can utilize digital signatures to track and sign electronic medical prescriptions, lab results, consent forms, and treatment plans [53]. By collecting the entity's digital signatures, any healthcare professional may determine whether the patient's medical data came from the intended entity. Some SHSs use sanitizable signatures to prevent changes in signed medical data. This ensures the integrity and validity of medical data, effectively hides sensitive patient information, promotes value-added medical information, and increases system efficiency. Other researchers have used dual signatures created using RSA, ECC, and hyperelliptic-curve cryptography to link two distinct sensitive types of medical information for two patients [153]. These digital signatures may be used online and offline to secure SHS and IoMT devices. Digital signatures guarantee the integrity, validity, and nonrepudiation of medical records, prescriptions, and other sensitive information. They also authenticate and authorize healthcare users, securely transmit information, sign prescriptions, manage consent and compliance, and enhance patient care and safety [53].

6.6 Anonymization

The IoMT devices, health mobile applications, and SHSs acquire and retain large amounts of sensitive patient medical records, diagnostic images, and genetic information, which must be kept secure from unauthorized access, abuse, and disclosure. Anonymizing medical data reduces the danger of reidentification while safeguarding the confidentiality of patients and sensitive health-related information. According to Andrew et al. [155] and Mosaiyebzadeh et al. [156], anonymization is the process of removing, substituting, distorting, generalizing, aggregating, or concealing patients' personally identifiable information from medical data stored in SHS while preserving the healthcare dataset's usability to protect their privacy and comply with regulations. Anonymization techniques are used to deidentify healthcare data by replacing patient-identifying information with pseudonyms while keeping the source of medical data anonymous. Anonymization must deidentify patient medical information before it is sent and analyzed [157]. This is accomplished by employing anonymization techniques such as pseudonymization, data masking, generalization, aggregation, randomization, noise addition, differential privacy, and encryption. Several anonymization solutions rely on the k-anonymity, l-diversity, and t-closeness models, which are popular anonymity protection strategies in smart healthcare [157]. In SHSs, anonymization provides several advantages, including protection of medical data privacy, healthcare data security, ethical use of medical data, facilitating medical research, fostering patient trust, guaranteeing compliance with healthcare regulations, long-term medical data utility, and driving innovation [157].

6.7 Key management-based solutions

The existing centralized SHS has numerous flaws, including data isolation, ownership, accountability, security, and privacy, and individuals do not have complete control over their medical information. Furthermore, smart healthcare includes intelligent medical equipment, wearable sensors, and IoMT devices, which makes identity management difficult for healthcare professionals. The centralized identity management system for smart healthcare has security, privacy, a single point of failure, and interoperability challenges, which can be solved using the decentralized identity management concept. Blockchain, a distributed technology, is critical in SHSs for storing patient medical information on a ledger. Since healthcare providers have been employing blockchain to record and maintain patient medical data, provide healthcare services, and securely store and share patient medical data online across several devices and platforms, key management

has become a significant problem. In smart healthcare, key management-based solutions use secure methods to manage cryptographic keys to encrypt and decrypt sensitive patient medical data in healthcare systems to ensure their confidentiality, integrity, and availability in digital settings. Medical professionals must swiftly access sensitive patient medical data in SHS via a master-key management and multikey server approach. Healthcare providers must maintain cryptographic keys securely, including the secret key and public/private key pairs. The core objective of key management is to create, distribute, and maintain keys until they are destroyed [158]. Key management processes involve key generation, distribution, storage, protection, rotation, revocation, and usage policies, including analyzing, assigning, creating, and distributing keys [53]. Key management strategies include security models based on key graphs and polynomial-based, tree-based, and chain-based key management. Key management techniques manage cryptographic keys in encryption, decryption, authentication, and other security applications. Some popular key management systems in smart healthcare include symmetric key management, public key infrastructure, key agreement schemes, key derivation schemes, key escrow, key revocation and rotation, attribute-based encryption, and homomorphic encryption. A key management scheme monitors healthcare systems by storing lifetime root keys in end devices. An intelligent healthcare monitoring system requires an end-to-end session key management scheme [53]. Effective key management in a cryptographic SHS ensures the confidentiality and integrity of transmitted medical data, lowers the risk of unauthorized medical data access, safeguards medical data transmitted between IoMT devices, and protects against potential cyber-attacks [47]. Wazid et al. [92] and Martínez et al. [47] cite other benefits, including patient privacy protection, healthcare data encryption, ensuring regulatory compliance, secure data sharing, access control, SHS auditing, and secure IoMT devices.

6.8 Authentication-based techniques

User authentication in SHS protects patient medical information from illegal access. Healthcare users, IoMT devices, and SHSs must all be verified using robust methods [99]. According to Da Silva et al. [159] and Alzu'bi et al. [160], authentication-based techniques are methods and technologies used to verify healthcare users' credentials against data stored in the system database and determine if the credentials match, ensuring that only authorized users have access to sensitive healthcare data and services. To prevent medical information from being disclosed to unauthorized entities, healthcare users and IoMT devices must be authenticated in SHSs [139]. Smart healthcare systems employ authentication procedures combining ownership, knowledge, and biometric factors to strengthen authentication [99] and implement authentication-based techniques such as usernames and passwords, biometric authentication, two-factor and multifactor authentication, smart cards and tokens, digital certificates, one-time passwords, risk-based authentication, certificate-based authentication, behavioral authentication, client-based user authentication, contextual-based access control, RFID authentication, location-based authentication, blockchain-based authentication, role-based access control, and advanced lightweight privacy-preserving authentication schemes to allow patients and healthcare providers to efficiently establish secure communications to healthcare systems and IoMT devices and ensure robust security [47][138][161][162]. Batista et al. [99] reported that wearables may authenticate the identities of healthcare users by collecting user-centric data such as heart rate, body temperature, electrocardiogram signals, and body motions. Combining these authentication-based techniques can improve the security and privacy of SHSs while protecting sensitive patient medical data from illegal access or breaches.

6.9 Strong access control-based techniques

The storage of large volumes of sensitive medical information in SHSs has led to numerous cyberattacks, making cybersecurity the top subject. To combat these cyber threats, healthcare providers must employ strong security and privacy solutions, such as strong access controls, to protect sensitive patient medical data and ensure the confidentiality, integrity, and availability of SHSs. According to Ahmed et al. [139], access control-based techniques are strategies such as consent, authentication, and authorization that are used in SHS and IoMT devices to control healthcare users' access to sensitive medical data, healthcare services, and IoMT devices, as well as the privileges granted to the users within a digital healthcare environment. Access control-based techniques must validate the party's identification and limit access to medical data, healthcare services, and IoMT devices while maintaining high security and privacy [85][99][151]. Some of the robust access control-based techniques used in SHSs include role-based access control, attribute-based access control, mandatory access control, biometric access control, blockchain-based access control, multifactor authentication, fine-grained access control, access control lists, and audit trails and logging [92][163][164]. The implementation of robust access control-based approaches guarantees that only authorized healthcare users can access or modify sensitive patient medical data [53][140][157][165]. Cryptographic techniques can safeguard access control mechanisms [99]. The implementation of robust access control-based techniques in SHSs has several benefits, including improving healthcare data confidentiality and integrity, protecting sensitive patient data from unauthorized access, ensuring regulatory compliance, mitigating insider threats, protecting IoMT devices and systems, enhancing accountability, improving operational efficiency, and fostering patient trust in SHSs [53][141].

6.10 Intrusion detection systems

Because of patient medical information sensitivity, fraudsters see SHSs, IoMT devices, and networks as lucrative targets. Intrusion detection systems are deployed to safeguard healthcare solutions, IoMT devices, servers, and healthcare users and to secure sensitive patient medical information [139]. Alhaj et al. [166] and Zubair et al. [93] defined an intrusion detection system as a security mechanism or control (i.e., hardware or software product) that monitors and analyzes network/system traffic and activities within a healthcare environment to detect and respond to potential anomalies, unauthorized access attempts, or suspicious activities. Intrusion detection systems have three components: information sources, analyses, and responses. Data from information sources are used in the analysis component to identify anomalies, and when an anomaly is detected, a response is initiated [167]. Intrusion detection systems can be network-based, which monitors data packets across the smart healthcare network for malicious activity, or host-based, which monitors all activities occurring within IoMT devices, servers, databases, and other system components [92]. When the healthcare system's usual behavior is described correctly, real-time activity is compared. Machine learning algorithms and behavioral analysis approaches detect unusual network behavior, whereas signature-based detection procedures identify previously known malicious activity patterns. When suspicious behavior is detected, the intrusion detection system sends real-time notifications to network administrators or security personnel [99]. Implementing intrusion detection systems in SHSs provides numerous benefits, including early threat detection, protection of patient medical data from unauthorized access, regulatory compliance, cyber-attack prevention, maintenance of SHS availability, anomaly detection, improved incident response, proactive risk management, and instant network traffic monitoring [37].

6.11 Security awareness and training

Because humans are considered the weakest link, smart healthcare providers must conduct regular training and awareness programs to educate healthcare professionals, patients, and other stakeholders about cyber threats and best security practices through lectures, seminars, and games [139][140][168]. Smart healthcare users need high-quality education and training programs that include up-to-date information, tips, recommendations, and campaigns that are simple to remember and apply to prevent healthcare user-related cyber-attacks. For example, healthcare users are trained on phishing attacks, patient rights, sensitive patient medical data security, SHS or end-user device security, IoMT device and application protection, the risks associated with data breaches and cyberattacks, and best security practices for strong login credentials and network and Wi-Fi security [141]. Training healthcare professionals and patients on best security practices and potential cyber threats in SHSs can help reduce human error, prevent security breaches caused by social engineering attacks, avoid unintended medical data leaks, reduce cybersecurity incidents, and improve patient safety and well-being [168].

6.12 Regular data backup

Healthcare providers are adopting and implementing comprehensive routine data backup and recovery procedures to preserve the privacy and security of medical data in SHSs and apps [50]. Regular data backups in SHSs are the systematic and planned process of creating and safely storing recent and accurate copies of medical information and ensuring that the information is easily restored during medical data loss, corruption, or system failure [139]. Healthcare providers can provide sensitive patient medical information both on-site and off-site. On-site backup maintains copies of sensitive medical information on physical hard drives and media and keeps them on-site for authorized personnel to quickly access in the event of a corruption, loss, system failure or natural disaster. Off-site backup involves storing medical information in a location other than the SHS environment, such as an off-site server, media devices, or the cloud [169]. Frequent backups of medical information should be encrypted and tested regularly to ensure their integrity and ability to be swiftly restored in the case of a ransomware attack, system failure, compromise, corruption, or data loss [140]. By establishing robust data backup in intelligent healthcare, healthcare providers can protect patient medical information, ensure robust security against system failure and malicious attacks, help healthcare practices become more efficient with their operations, maintain the continuity of healthcare services, help healthcare providers become more compliant with regulations like HIPAA, reduce the costs associated with data loss, increase competitive advantage, make it easier to manage and restore data, ensure efficient use of resources, reduce workloads, safeguard patient welfare, support high-quality healthcare services, ensure recovery from ransomware attacks and data loss incidents, and help archive and preserve medical information for future reference [140][170].

6.13 Network security

With the growing global use of SHSs, providing strong network security is critical for protecting sensitive patient medical information and maintaining the overall integrity of healthcare operations. The Internet of Medical Things devices, patient medical data, and secure communication networks are connected to improve patient care, efficiency, and accessibility in SHSs [35]. In an SHS, network security refers to security measures and protocols implemented to safeguard the integrity,

confidentiality, and availability of medical data and communication within the healthcare system that provides healthcare services via smart devices, IoMT devices, and networks [43]. Several security measures, such as secure communication channels, data encryption, access control, firewalls, intrusion detection/prevention systems, physical security, regular security audits and updates, endpoint security, data loss prevention, network segmentation, employee training and awareness, and incident response plans, are used to monitor and control network traffic to SHSs, prevent unauthorized access to patient medical information, and safeguard against cyber-attacks [35][139][141]. The implementation of robust network security measures in SHSs has several advantages, including reducing data breaches, protecting patient medical data confidentiality and integrity, preventing unauthorized access, maintaining IoMT device integrity, preventing malware and cyberattacks, ensuring healthcare service continuity, complying with regulations, improving trust and reputation, and saving money.

6.14 Network segmentation

In smart healthcare, networked medical equipment, IoMT devices, and intelligent systems are used to share medical data and enhance patient care. These systems and devices are vulnerable to online attacks. Network segmentation is critical for reducing cyber-attacks in healthcare networks by integrating network Layers 2 and 3 techniques such as virtual local area networks, access control lists, subnetting, and firewalling. In smart healthcare, network segmentation is a security practice and defense-in-depth strategy that involves splitting a healthcare organization's network into multiple smaller subnetworks or zones to protect sensitive medical data, reduce congestion, limit system failures, and limit access to the rest of the network [171]. Each segment in an intelligent healthcare setting serves as an extra security layer with access points, login credentials, and firewall protection separated from the others, forming barriers that prevent unauthorized access to SHSs, separating IoMT devices from the rest of the IT, medical devices and services that help in monitoring patients in real-time and remotely and restricting the spread of cyber threats [22]. By implementing a network segmentation policy, smart healthcare providers can control the spread of a cyber-attack and limit the damage caused, provide better access control to network security, improve the flow of traffic between networks, easier network traffic monitoring and threat detection, improve the performance and reliability of the smart healthcare network, better protect sensitive medical data and endpoint devices, reduce the impact of a successful cyberattack, enhance compliance with regulations and standards, such as HIPAA, and secure cloud-based servers [140].

6.15 Patch management

Cyberattacks on smart healthcare networks expose sensitive patient medical data, betray patients' trust, and even cause human death. The most effective method is to apply security patches to SHSs to identify vulnerabilities, preserve the integrity, confidentiality, and availability of patient medical data, and ensure the reliability of intelligent healthcare services [172]. Patch management in a SHS is the multifaceted process of identifying, acquiring, testing, and deploying software patches and updates to computers, operating systems, network infrastructure, gateways, medical devices, SHS, and IoMT devices to address vulnerabilities and improve security and functionality [139][172]. The patches include bug fixes, software and security upgrades, and feature additions or enhancements. Patch management processes include patch information collection, vulnerability scanning, assessment and prioritization, patch testing, patch deployment, and postdeployment patch verification [172]. Routine and thorough patching of SHSs can protect them from emerging cyber threats while improving overall system performance, healthcare delivery efficiency, and safety [139]. Some advantages of implementing patch management in SHSs include maintaining the security, reliability, and efficiency of SHS and IoMT devices; avoiding penalties and fines; smoothing the healthcare user experience; enhancing the features, usability, and performance of the SHS; contributing to better patient care and outcomes; and protecting healthcare systems from known vulnerabilities [141][172].

6.16 Data loss prevention

Smart healthcare systems include sensitive patient health records, digital medical records, genomic data, medical imaging data, continuous monitoring data, telemedicine and telehealth data, clinical notes and documentation, administrative and billing data, drug and treatment data, population health data, research and clinical trial data, and security and access logs generated and processed by IoMT devices, smart devices, wearable devices, and telemedicine platforms. These data are exchanged across healthcare providers and stakeholders, resulting in enormous loss and leakage. This violates patient privacy, damages healthcare providers' reputations, and leads to lawsuits and regulatory infractions. Therefore, there is a high demand for data loss prevention in SHSs. Data loss prevention includes security measures and technologies that identify and protect sensitive patient medical information stored in on-premises systems, cloud-based locations, and endpoint devices and shared from unauthorized access, disclosure, or loss. The data loss prevention strategies used in smart healthcare environments include encryption, access controls, data classification, data masking, user activity monitoring, network security, endpoint security, data backup and recovery, employee training and awareness, regulatory compliance,

and continuous monitoring and improvement [139]. It is vital in SHSs because it protects patient privacy, prevents sensitive medical data breaches, complies with regulations such as the HIPAA and GDPR, manages risk and incident response, prevents unauthorized access to medical data, improves data governance, optimizes healthcare operational efficiency, ensures the integrity and confidentiality of sensitive medical information, and protects intellectual property.

6.17 Regular security audits and testing

With the increasing number of cyber threats to SHSs, it is paramount to keep security measures up to date and undertake frequent security audits and testing to detect possible systems and network architecture vulnerabilities. According to Agrawal et al. [173], regular security audits are proactive strategies for identifying and fixing vulnerabilities and flaws in SHSs, IoMT devices, and network infrastructure before cybercriminals exploit them. Regular security audits and penetration testing improve the security of SHSs, ensuring robust defenses against potential cyberattacks and protecting sensitive patient medical data [50][173]. Furthermore, periodic third-party vendor audits are crucial in smart healthcare networks because they have access to sensitive patient medical information, and assessing vulnerabilities is required to implement fixes and ensure that they meet strict cybersecurity standards [139][140]. Security audits and testing for smart healthcare networks and systems include vulnerability assessments, compliance checks, penetration testing, vulnerability scanning, access logs and code review, security configuration review, security incident response testing, security awareness training, continuous network traffic monitoring, and third-party assessments [141]. They are essential because they help to ensure sensitive medical data integrity and confidentiality, guarantee the proper functioning of the SHS, track system and healthcare user activities, identify and address potential system vulnerabilities and security incidents, and ensure adherence to industry standards and regulations [22][142][174][175].

6.18 Incident response plan

With the interconnection of networks, medical equipment, IoMT devices, and data repositories, SHSs can improve patient care and operational efficiency. However, these systems are vulnerable to numerous cyber threats. The development of a detailed incident response plan permits healthcare providers to respond swiftly and efficiently in the case of a security breach by separating compromised systems, alerting concerned authorities, and starting recovery processes. An incident response plan is a collection of organized techniques, strategies, policies, and hardware and software security solutions that healthcare providers use to manage and alleviate security incidents, data leakages, and breaches in their digital infrastructure. Smart healthcare providers must develop an incident response plan that outlines the steps for detecting, responding to, and recovering from security breaches, incidents, and unauthorized system and network access, as well as the responsibilities of people or teams in handling and mitigating incidents [176]. These steps include preparation, detection and analysis, containment, eradication, recovery, post-incident analysis, and communication [140]. Healthcare providers must develop an incident response strategy before the event occurs and secure all indications, detection procedures, and analytical approaches. A robust and coordinated response to security incidents alleviates the impact, while patient care is undisturbed [173]. Incident response plans are essential in smart healthcare because they reduce SHS downtime, detect and respond to security incidents, reduce financial loss, ensure that healthcare providers comply with regulations, improve stakeholder confidence and effective resource allocation, improve recovery time, and continuously improve the security posture.

6.19 Continuous monitoring and detection of anomalies

With the healthcare industry's rapidly expanding cyber threat landscape, continuously monitoring and detecting threats and vulnerabilities in SHSs is critical. Healthcare providers must be aware and practical in detecting and reducing cyber risks as they arise [173]. Continuous monitoring and anomaly detection include collecting, analyzing, and interpreting multiple data points on healthcare systems instantly to find deviations from expected patterns or behaviors. Healthcare providers can use behavioral analytics to identify abnormal patterns of activity that may indicate a security compromise, and these anomalies can be linked to data or smart healthcare and IoMT networks [177]. Smart healthcare systems, IoMT apps, and device-related logs are collected continually to monitor smart healthcare networks and detect cyber threats. Logs can be monitored, analyzed, and evaluated to avoid security issues using artificial intelligence, machine learning, and deep learning techniques [85]. These anomalies must be identified instantaneously on local networks or cloud servers, with no false alarms, and continuous monitoring systems must be capable of detecting and responding to irregularities immediately [177]. Intrusion detection/preventive systems, security information and event management tools, and real-time log analysis all help quickly identify and mitigate attacks [139][140]. Data collection, integration, analytic techniques, real-time monitoring, alerting systems, response and intervention, feedback loops, and security and privacy are all components of continuous monitoring and anomaly detection. Early warning of possible threats allows healthcare providers to respond more readily and organize their actions more efficiently [78]. Continuous monitoring and anomaly detection in the SHS

provides benefits such as improved patient outcomes and safety, increased efficiency and cost-effectiveness in healthcare delivery, and the ability to identify and respond quickly to cybersecurity incidents [139][140].

6.20 Regular risk assessment

The success of an intelligent healthcare business depends on cybersecurity, and security estimation is crucial for assessing its performance and protection level. However, several cyber threats in the healthcare industry can compromise hardware and software vulnerabilities that endanger medical information availability, privacy, integrity, and confidentiality [178]. As a result, frequent risk assessments of cyber threats in SHSs are conducted and evaluated to manage and mitigate cyber risks. According to Ksibi et al. [179] and Pritika et al. [180], regular risk assessment is a comprehensive process that includes identifying security threats, examining the vulnerabilities of SHSs, and evaluating the impact of security breaches on the system and network. Regular risk assessments allow healthcare providers to identify areas of vulnerability within the SHS and network, optimize resources, and apply preventive measures to limit the probability and severity of adverse events. It involves identifying, analyzing, mitigating, monitoring, and reviewing risks, ensuring regulatory compliance, training, and developing incident response plans [178]. The risk assessment process aims to understand potential risks in smart healthcare by estimating and rating their severity before attempting to mitigate them [180]. The two regular risk assessment methodologies include qualitative and quantitative methods. A qualitative risk assessment scores the likely consequences of the linked incidence as high, medium, or low. Quantitative risk assessment uses numerical values to rank the consequences and related probabilities [178][179]. Operationally critical threat, assets, and vulnerability evaluation (OCTAVE), a qualitative risk assessment method, is used for information system risk assessment. It evaluates typical security and privacy vulnerabilities in SHS [178]. These methodologies involve risk assessment and management phases [181]. Risk assessment frameworks in smart healthcare include the (1) National Institute of Standards and Technology (NIST) Framework, (2) International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 Cybersecurity Framework, (3) Threat Analysis and Risk Assessment (TARA) Framework, (4) Factor Analysis of Information Risk (FAIR), and (5) Institute of Electrical and Electronics Engineers (IEEE) 2413-2019 (P2413) Standard [180]. Regular risk assessment in the SHS offers several benefits, such as enhanced smart healthcare security by identifying vulnerabilities and weak entry points for cyberattacks, improved regulatory compliance within healthcare providers, reduced financial loss, protection of patient privacy, increased patient trust and confidence, efficient resource allocation, continuous improvement, improved quality of patient care and outcomes, and early detection of emerging risks [140][180][182].

6.21 Threat intelligence sharing

The smart healthcare system relies on networked IoMT devices, medical equipment, networks, and data to improve patient care, operational efficiency, and outcomes. Nonetheless, the increased connection between devices raises cyber threats. Healthcare providers must use cyber threat intelligence sharing strategies to stay ahead of cybercriminals. This allows them to better understand threat incidents and make informed decisions about security approaches by sharing potential and existing cyber threat information with other organizations, individuals, or entities. Threat intelligence in smart healthcare refers to the collection, transformation, observation, analysis, and interpretation of any information or knowledge about cyber threats or attacks that will assist healthcare providers in taking appropriate action to protect their healthcare systems and networks [183]. Zhang et al. [184] and Ali et al. [185] define threat intelligence sharing as a proactive approach in which security experts in healthcare organizations collaborate to share insights and information about suspicious activities, potential cyber threats, attack patterns, and threat incidents with only trusted partners to enhance the entire security of the SHS and network. Threat intelligence information is gathered from internal network logs, security tools, open-source intelligence, commercial threat intelligence feeds, and industry-specific sharing networks such as information sharing and analysis centers. Security professionals must analyze the acquired data to uncover trends and practical intelligence to help healthcare providers understand the threat scene and make informed security decisions. Smart healthcare systems use intrusion detection systems, firewalls, security information and event management solutions, and anomaly detection algorithms to quickly identify potential security incidents, suspicious activity and unauthorized access attempts [183]. Threat intelligence employs the information gathered through the security techniques mentioned above to determine threat or attack patterns [183]. Healthcare providers must work with industry peers, government agencies, and cybersecurity organizations to share threat intelligence information and stay current on new cyber threats, vulnerabilities, and best practices to collectively defend SHSs and networks [140]. Information sharing and analysis centers and health information sharing and analysis centers provide collaborative platforms for stakeholders to share threat intelligence that is relevant, actionable and valuable [183]. The threat intelligence sharing process consists of (1) collecting threat intelligence, (2) analyzing the collected data to identify patterns, (3) standardizing the data structure using standardized formats and languages, (4) sharing threat intelligence, (5) reviewing shared intelligence, and (6) monitoring the effectiveness of threat intelligence sharing efforts and providing feedback to partners. The significance of threat intelligence sharing in smart

healthcare includes early threat detection, improved incident response, cost savings, improved regulatory compliance, participants provided with awareness and training materials and support, cost-effective tools in fighting cybercrime, collaborative defense, patient data protection, building solid relationships with industry partners, and encouraging collaboration by combining resources, knowledge, and expertise, innovation support, enhanced comprehension of threat actors and their strategies, approaches, and processes, and ensuring the security and integrity of patient data, IoMT devices, medical equipment, and healthcare infrastructure [186].

6.22 Blockchain-based privacy preservation techniques

Centralized healthcare service systems cannot meet the growing demand for exchanging patient medical data across many healthcare departments. This calls for the use of blockchain technology in SHSs to decentralize the management of massive amounts of medical data through distributed ledgers. It also allows healthcare users to perform transactions without the involvement of third parties, allowing patients to easily access, securely share, and protect their privacy and security [187]. Blockchain features such as decentralization, transparency, open sources, autonomy, immutability, irreversibility, and anonymity have emerged as solutions to decentralization and security issues in the smart healthcare sector [157][188]. A distributed shared ledger keeps and manages patient medical data through consensus across blockchain network nodes. The hash function generates the message digest of the previous block in the newly formed block, and the blocks form a chain structure that is successively linked and subsequently recorded in the blockchain. The blockchain stores verified medical data that cannot be edited or removed randomly. The shared ledger protects blockchain blocks using cryptographic methods, ensuring medical data integrity, transparency, and privacy [110][185]. Blockchain improves the interoperability of existing medical records by using an immutable database and masking user identity via public key transactions. It also provides a safe and trustworthy method for storing and retrieving patient medical information. The significance of using blockchain-based privacy preservation techniques in SHSs includes improving medical data security, integrity, and patient confidentiality; enhancing patient trust and engagement; ensuring patient control over medical data; enabling interoperability and cross-domain medical data sharing; compliance with regulations; removing third parties; facilitating medical research and innovation; assisting patients to exercise their access rights; immutable patient medical records audit trails; improving medical data scalability; ensuring fault tolerance and transparency; ensuring medical data encryption and decentralization; delivering comprehensive healthcare services; and ensuring that medical data are verifiable and not tampered with [188].

6.23 Machine learning solutions

The incorporation of wearable, IoMT, medical, and other smart devices into SHSs and networks has facilitated the easy transfer of patient medical data across medical devices, increased patient care quality, and improved remote patient monitoring. However, cyber threats and attacks jeopardize the medical data acquired by many medical sensors and smart devices, causing patients to lose trust in the system. Despite these cyber threats and attacks, machine learning could improve cybersecurity by altering the understanding, classification, and response to cyber-attacks by identifying abnormalities or patterns in medical data and networks [189-191]. This practical strategy enables healthcare providers to take preventive measures to mitigate damage and prevent medical data breaches. In SHSs and networks, machine learning uses algorithms and statistical models to improve computer system performance on specific tasks over time. It can examine network traffic for unusual patterns and identify cyber-attacks such as MiTM attacks, zero-day attacks, data injection, DDoS attacks, and spoofing [192]. Machine learning algorithms are classified as supervised, semisupervised, or unsupervised [191]. Support vector machines, decision trees, random forests, K-means algorithms, K-means clustering, artificial neural networks, K-nearest neighbors, decision trees, deep neural networks, Q-learning, naive Bayes, deep learning algorithms, recurrent neural networks, and principal component analysis are examples of machine learning algorithms used to improve cybersecurity in smart healthcare. These machine learning techniques help in analyzing massive medical datasets to effectively and efficiently detect anomalies, provide predictive analytics for threat detection, detect fraud and intrusion, manage and automate security, detect malware, provide security education and awareness, ensure secure authentication, manage vulnerabilities, privacy-preserving data sharing, provide threat intelligence and automated response, monitor medical data to identify traffic modifications, and provide network and adaptive security measures [167][193]. These solutions provide numerous benefits for improving cybersecurity in SHSs, such as early threat detection, adaptive defense mechanisms, reduced false positives, improved fraud detection, better access control, privacy-preserving data analysis, predictive security analytics, streamlined compliance management, improved effectiveness of security measures, cost-efficiency, and improved intrusion detection and response systems' ability to detect and respond to possible threats [192].

6.24 Physical security

As healthcare technology and solutions evolve, the cybersecurity environment in IoMTs and medical devices, SHSs, and networks expands, posing significant challenges and threats to healthcare providers, professionals, and patients. To protect

patients, healthcare providers must adopt measures such as physical security. Physical security refers to various methods and processes designed to secure physical assets, infrastructure, IoMT devices, medical equipment, buildings, and sensitive medical data while providing healthcare services and protecting patients and healthcare personnel. It is critical in SHSs due to sensitive patient medical data and the potential risks of illegal access [194]. Healthcare providers must use physical security measures such as alarms, access control systems, ID badges, surveillance cameras, locks, motion sensors, and others to prevent unauthorized access and damage to servers, computers, IoMTs and medical devices that store patient data [98]. To ensure robust physical security, healthcare providers must implement access control, surveillance systems, perimeter security, data center security, device security, disaster preparedness, regular audits and assessments, staff training, vendor management, physical asset management, and regulatory compliance. Physical security in the SHS is crucial because it safeguards patient information and privacy, prevents unauthorized access to medical and IoMT devices, ensures healthcare continuity, mitigates insider threats, secures the SHS, prevents physical theft and vandalism, detects intrusions, improves disaster preparedness and response, and fosters patient trust and confidence [195].

6.25 Regulatory compliance

As the SHS transforms the healthcare domain, it benefits patients, healthcare providers and professionals. However, its implementation faces obstacles, particularly in terms of regulatory compliance. Regulatory compliance occurs when healthcare providers, technology providers, and other healthcare stakeholders follow the laws, regulations, standards, and rules established by regulatory bodies and authorities for developing, deploying, and using IoMT devices and SHSs; upholding legal and ethical standards; protecting patients and the healthcare environment; and promoting fair competition. It is a continual process that requires active participation from healthcare professionals to improve the general quality of healthcare and strict processes to eliminate mistakes and malpractice, hence boosting healthcare providers' credibility. Examples of regulations in smart healthcare are the HIPAA, the GDPR, the Health Information Trust Alliance Security Framework, Cybersecurity Standards (e.g., ISO/IEC 27001, ISO/IEC 82304, ISO/IEC 62304, ISO 25237:2017, ISO/IEC 27701, ISO/IEC 27002), Medical Standards (e.g., IEC 62304:2006, ISO/IEC 27032:2012, IEC 82304-1:2016, IEC/TR 80002-1:2009, ISO/TR 80002-2:2017, IEC/TR 80002-3:2014), Interoperability Standards (e.g., Fast Healthcare Interoperability Resources), and medical device regulations (e.g., European Union's Medical Device Regulation, Food and Drug Administration) [141][173][196-200]. These laws necessitate extensive documentation, stringent quality control procedures, frequent audits, and adherence to particular protocols throughout production and distribution operations. Healthcare regulations establish strict data collection, storage, and sharing standards to safeguard patient rights and maintain medical data security. To comply with legal requirements, healthcare organizations must prioritize medical data governance, build robust security procedures, and implement rigorous access restrictions [173]. Privacy and data security, interoperability standards, medical device regulations, ethical concerns, quality and safety standards, regulatory reporting and documentation, and ongoing monitoring and compliance updates are all aspects of regulatory compliance in smart healthcare. Regulatory compliance in smart healthcare has numerous advantages, including patient safety and privacy, medical data integrity, risk mitigation, interoperability, improved healthcare quality, increased patient trust and healthcare provider reputation, enabling innovation, cost savings, increased patient and healthcare user engagement, and regulatory alignment [199].

Healthcare providers may strengthen their cybersecurity posture by deploying the security strategies discussed above that improve patient medical data protection, IoMT devices, and critical smart healthcare devices and networks. These measures must be updated regularly to maintain robust cybersecurity in a smart healthcare setting, emphasizing evolving cyber threats and technology.

7. THE ROLE OF CYBERSECURITY IN SUSTAINING SMART HEALTHCARE

Cybersecurity is a diverse and crucial component of ensuring the sustainability and performance of smart healthcare systems. The essential roles of cybersecurity in ensuring the sustainability of smart healthcare include the following [39][40]:

- *Patient data protection*: Smart healthcare systems rely primarily on collecting and analyzing patient data for individualized treatment. This includes sensitive information such as medical history, test results, and treatment plans. Effective cybersecurity measures are required to protect these data from illegal access while maintaining patient privacy and confidentiality.
- *Preventing data breaches*: Healthcare data breaches can have significant repercussions, such as financial losses, reputational harm, and compromised patient safety. Encryption, access restrictions, and intrusion detection systems are examples of cybersecurity solutions that can help prevent unwanted access to healthcare systems and reduce the risk of data breaches.

- *Maintaining SHS integrity and availability*: Cyber attacks can impair the availability and operation of intelligent healthcare systems, possibly jeopardizing patient care. Healthcare providers may protect the integrity and availability of vital systems and services by implementing cybersecurity measures, including network monitoring and system backups.
- *Preventing malicious attacks*: Smart healthcare systems are susceptible to various cyber threats, such as ransomware, phishing, and malware. Employee training, threat intelligence, and vulnerability assessments all contribute to detecting and mitigating these threats, lowering the risk of malicious attacks.
- *Compliance with regulations*: Healthcare firms must adhere to severe regulatory standards for patient data protection, such as the HIPAA in the United States and the GDPR in the European Union. Adherence to these requirements necessitates strong cybersecurity measures to preserve patient information and avoid regulatory fines.
- *Ensuring Trust and Confidence*: Patients must believe that their healthcare professionals will secure sensitive information. A strong cybersecurity strategy involves a commitment to protecting patient data and building trust in innovative healthcare technologies.
- *Protection of patient privacy*: Smart healthcare systems safeguard patient privacy by limiting access to medical records and ensuring that sensitive information is available only to authorized individuals.
- *Vendor risk management*: Healthcare providers usually hire third-party vendors to develop SHSs. Healthcare providers must assess and manage cybersecurity risks linked with third-party vendors and providers offering IT services or products to healthcare organizations.
- *Risk management*: Cybersecurity assists in identifying, assessing, and mitigating risks associated with possible cyberattacks and vulnerabilities in healthcare IT systems.
- *Smart healthcare network security*: Smart healthcare networks defend intelligent healthcare networks from cyber threats, including malware, ransomware, and unauthorized access attempts, which might disrupt operations and jeopardize patient data.
- *Smart healthcare user identity and access management*: Cybersecurity implements strong identity and access management systems to govern access to sensitive SHSs and data, guaranteeing that only authorized personnel can access them.
- *Ensuring continuity of care*: By safeguarding against cyberattacks and ransomware, cybersecurity contributes to the continuity of healthcare services, reducing disruptions that might impact patient care.
- *Protecting telehealth and IoMT devices*: With the growing usage of telehealth and IoMT devices in healthcare, cybersecurity is critical for securing these endpoints and preventing possible vulnerabilities from being exploited.
- *Secure healthcare software development*: Cybersecurity encourages secure healthcare software development methods to create strong and resilient healthcare apps and systems from the start.
- *Incident response*: It sets rules and processes for quickly responding to cybersecurity issues, minimizing their impact on patient care and organizational operations.
- *Continuous monitoring*: In smart healthcare, constant monitoring involves continuous monitoring of healthcare IT infrastructure and networks for possible security risks or abnormalities, allowing for proactive threat identification and response.
- *Interoperability security*: Cybersecurity addresses security issues associated with interoperability among various healthcare systems and platforms, guaranteeing secure data flow and communication.
- *Facilitating innovation*: Cybersecurity facilitates healthcare innovation by providing a safe environment for data exchange and collaboration and promoting innovative technology and solutions that enhance patient outcomes.
- *Protecting research and development*: Cybersecurity protects intellectual property, research discoveries, and proprietary information connected to healthcare innovation against theft or compromise.
- *Collaboration and information sharing:* This initiative encourages healthcare providers, cybersecurity specialists, and government agencies to work together to build cybersecurity defenses and respond effectively to emerging threats.

Cybersecurity contributes to the sustainable development and advancement of SHSs by performing these roles, thus ensuring that they are robust, trustworthy, and capable of providing high-quality care while preserving patient privacy and safety.

8. CONCLUSIONS

The cybersecurity landscape within sustainable smart healthcare has emerged as a top priority. It is densely braided with complexities and nuances that require utmost attention and creative thinking. Researchers have comprehensively explored state-of-the-art methods, methodically constructed a taxonomy of cybersecurity threats in smart healthcare ecosystems, examined security mechanisms, and highlighted the critical roles of cybersecurity in ensuring sustainable smart healthcare. The multiple facets of cybersecurity in smart healthcare reveal progress and formidable problems ahead. As technology advances in smart healthcare, so do cyber threats and attacks, demanding continuous adaptation and vigilance.

This study emphasizes the critical responsibilities that diverse stakeholders must play in ensuring the integrity and resilience of smart healthcare systems. From lawmakers developing rigorous rules to healthcare providers adopting strict policies,

cybersecurity specialist hardening defenses, and technology developers integrating security by design, each stakeholder plays a vital role in cybersecurity technology for long-term smart healthcare.

However, despite the complexity, there is a ray of hope in commitment to innovation, collaboration, and the quest for a safer, more resilient future. By using technology, knowledge, and social action, the foundations of smart healthcare can be strengthened, ensuring its continued sustainability and security. The researchers believe that the path to sustainable smart healthcare is related to the objective of cybersecurity excellence. By applying the insights gained from this review and accepting cybersecurity as a fundamental pillar of sustainable healthcare, researchers can confidently navigate the complexities of the digital age, ensuring that the promise of smart healthcare is realized in a secure, resilient, and equitable manner for all.

In the future, potential cyber threats and attacks such as data breaches, ransomware attacks, IoT device vulnerabilities, malware targeting medical devices, insider threats, supply chain attacks, social engineering attacks, DoS attacks, and regulatory compliance challenges will persist. This calls for research focusing on advanced threat detection and response, privacy-preserving technologies, behavioral analytics, interoperability and standards, advanced cryptography such as quantum cryptography, touchless access control solutions, the use of artificial intelligence and machine learning, human factors and training, and regulatory compliance governance to counteract threats.

Funding

The authors had no institutional or sponsor support.

Conflicts of interest

The author's disclosure statement confirms the absence of any conflicts of interest.

Acknowledgment

The authors thank the institutions for their unwavering support and encouragement during this research.

References

[1] Z. Tang, L. Jiang, X. Zhu, and M. Huang, "An Internet of Things-Based Home Telehealth System for Smart Healthcare by Monitoring Sleep and Water Usage: A Preliminary Study," *Electronics*, vol.12, no.17, pp.1-14, August 2023. https://doi.org/10.3390/electronics12173652

[2] M. A. Elhosseini, N. K. Gharaibeh and W. A. Abu-Ain, "Trends in Smart Healthcare Systems for Smart Cities Applications," In Proceedings of International Conference on Advanced Innovations in Smart Cities (ICAISC), Jeddah, Saudi Arabia, 23-25 January 2023, pp.1–7. https://doi.org/10.1109/icaisc56366.2023.10085212

[3] A. Wells and A. B. Usman, "Privacy and biometrics for smart healthcare systems: attacks, and techniques," *Information Security Journal: A Global Perspective*, vol.33, no.3, pp.307–331, October 2023. https://doi.org/10.1080/19393555.2023.2260818

[4] F. Bu, M. Wang, and L. "Tian, Research on Medical Big Data Mining and Intelligent Analysis for Smart Healthcare," In proceedings of International Conference on 3D Immersion, Interaction and Multi-sensory Experiences (ICDIIME), Madrid, Spain, 27-29 June 2023, pp.394–39. https://doi.org/10.1109/icdiime59043.2023.00082

[5] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. Shetty, and A. Alqahtani, "Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications," *IEEE Access*, vol.11, pp.93032–93047, August 2023. https://doi.org/10.1109/access.2023.3310264

[6] G. Sandi, S. H. Supangkat, Ermawati, "Smart Healthcare for Personalized Healthcare: Literature Review," In Proceedings of International Conference on ICT for Smart Society (ICISS), Bandung, Indonesia, 06-07 September 2023, pp.1–7. https://doi.org/10.1109/iciss59129.2023.10291631

[7] M.-H. Lee, I-H. Liu, and J.-S. Li, "Cyber Security in a 5G-Based Smart Healthcare Network: A Base Station Case Study," Engineering Proceedings, vol.55, no.1, pp.1-6, December 2023. https://doi.org/10.3390/engproc2023055050

[8] M. Wazid, S. Thapliyal, D. P. Singh, A. K. Das, and S. Shetty, "Design and Testbed Experiments of User Authentication and Key Establishment Mechanism for Smart Healthcare Cyber-Physical Systems," *IEEE Transactions on Network Science and Engineering*, vol.10, no.5, pp.2697–2709, March 2022. https://doi.org/10.1109/tnse.2022.3163201

[9] Statista. "Digital Health - Worldwide." Statista. https://www.statista.com/outlook/hmo/digital-health/worldwide#revenue (accessed January 5, 2024).

[10] AH. Al-Mistarehi, M. M. Mijwil, Y. Filali, M. Bounabi, G. Ali, and M. Abotaleb, "Artificial Intelligence Solutions for Health 4.0: Overcoming Challenges and Surveying Applications," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol.2023, pp.15–20, March 2023. https://doi.org/10.58496/mjaih/2023/003

[11] R. Natarajan, G. H. Lokesh, F. Flammini, A. Premkumar, V. K. Venkatesan, and S. K. Gupta, "A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0," *Infrastructures*, vol.8, no.2, pp.1–18, 2023. https://doi.org/10.3390/infrastructures8020022

[12] L. Gomathi, A. K. Mishra, and A. K. Tyagi, "Industry 5.0 for Healthcare 5.0: Opportunities, Challenges and Future Research Possibilities," In the Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11-13 April 2023 https://doi.org/10.1109/icoei56765.2023.10125660

[13] M. A. Salman and M. A. Mahdi, "Multi-Strategy Fusion for Enhancing Localization in Wireless Sensor Networks (WSNs)," *Iraqi Journal for Computer Science and Mathematics*, vol.5, no.1, pp.299–326, 2024. https://doi.org/10.52866/ijcsm.2024.05.01.021

[14] H. Alasmary, "ScalableDigitalHealth (SDH): An IoT-Based Scalable Framework for Remote Patient Monitoring," *Sensors*, vol.24, no.4, pp.1–14, February 2024. https://doi.org/10.3390/s24041346

[15] M. M. Mijwil, I. Bala, G. Ali, M. Aljanabi, M. Abotaleb, R. Doshi, K. K. Hiran and E.-S. M. El-Kenawy, "Sensing of Type 2 Diabetes Patients Based on Internet of Things Solutions: An Extensive Survey," in *Modern Technology in Healthcare and Medical Education: Blockchain, IoT, AR, and VR*, Ed. Hampshire: IGI Global, 2024, pp. 34-46. https://doi.org/10.4018/979-8-3693-5493-3

[16] M. Humayun, A. Alsirhani, F. Alserhani, M. Shaheen, and G. Alwakid, "Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency," *Journal of Cloud Computing*, vol.13, no.1, pp.1–21, 2024. https://doi.org/10.1186/s13677-024-00602-2

[17] Y. Zhu, J. Li, J. Kim, S. Li, Y. Zhao, et al., "Skin-interfaced electronics: A promising and intelligent paradigm for personalized healthcare," *Biomaterials*, vol.296, pp.122075, 2023. https://doi.org/10.1016/j.biomaterials.2023.122075

[18] N. Kumar and R. Ali, "A smart contract-based robotic surgery authentication system for healthcare using 6G-Tactile Internet," *Computer Networks*, vol.238, pp.110133, 2024. https://doi.org/10.1016/j.comnet.2023.110133

[19] C. M. Roberts, J. M. Plevinsky, K. L. Gamwell, A. E. Noser, L. A. Denson, and K. A. Hommel, "Self-Management assistance for recommended treatment (SMART) IBD app randomized control trial in adolescents with IBD: Design and methodology," *Health Care Transitions*, vol.2, pp.1–6, 2024. https://doi.org/10.1016/j.hctj.2023.100031

[20] K. Al-Naime, A. Al-Anbuky, and G. Mawston, "Internet of Things Gateway Edge for Movement Monitoring in a Smart Healthcare System," *Electronics*, vol.12, no.16, pp.1-13, August 2023. https://doi.org/10.3390/electronics12163449

[21] S. M. H. Fard, V. Agrawal, F. Gebali, H. Elmiligi, and M. S. I. Mamun, "Ensemble Siamese Network (ESN) Using ECG Signals for Human Authentication in Smart Healthcare System," *Sensors*, vol.23, no.1, pp.1-14, May 2023. https://doi.org/10.3390/s23104727

[22] M. F. Javed, N. Tariq, M. I. Ashraf, F. A. Khan, M. Asim, and M. Imran, "Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework," *Sensors*, vol.23, no.23, pp.1-45, November 2023. https://doi.org/10.3390/s23239372

[23] A. Dhawan, "Taking Preventive Action to Reduce Cybersecurity Risks in IOT-Based Smart Healthcare Networks," In Proceedings of International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 12-13 May 2023, pp.2370–2374. https://doi.org/10.1109/icacite57410.2023.10182865

[24] I. Albarazanchi, H. Abdulshaheed, M. M. Abdulrahman, and J. F. Tawfeq, "Identification of Faulty Sensor Nodes in WBAN Using Genetically Linked Artificial Neural Network," *Iraqi Journal for Computer Science and Mathematics*, vol.5, no. 2, pp.48–58, 2024. https://doi.org/10.52866/ijcsm.2024.05.02.005

[25] A. Habbal, M. Ali, and M. A. Abuzaraida, "Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions," *Expert Systems With Applications*, vol.240, pp.1–14, 2024. https://doi.org/10.1016/j.eswa.2023.122442

[26] N. I. C. Mat, N. Jamil, Y. Yusoff, and L. M. Kiah, "A systematic literature review on advanced persistent threat behaviors and its detection strategy," *Journal of Cybersecurity*, vol.10, no.1, pp.1–18, 2024. https://doi.org/10.1093/cybsec/tyad023

[27] K. S. Niksirat, L. Velykoivanenko, N. Zufferey, M. Cherubini, K. Huguenin, and M. Humbert, "Wearable Activity Trackers: A Survey on Utility, Privacy, and Security," *ACM Computing Surveys*, vol.1, no.1, pp.1–41, 2024. https://doi.org/10.1145/3645091

[28] R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "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*, vol.35, no.1, pp.1–48, 2024. https://doi.org/10.1002/ett.4884

[29] L. Alzubaidi, K. Al-Dulaimi, H. A. Obeed, A. Saihood, M. A. Fadhel, S. A. Jebur, Y. Chen, A. S. Albahri, J. Santamaría, A. Gupta, and Y. Gu, "MEFF - A Model Ensemble Feature Fusion Approach for Tackling Adversarial Attacks in Medical Imaging," *Intelligent Systems With Applications*, vol.22, pp.1–20, 2024. https://doi.org/10.1016/j.iswa.2024.200355

[30] L. Da Costa, B. Pinheiro, W. Cordeiro, R. Araújo, and A. Abélem, "Sec-Health: A Blockchain-Based Protocol for Securing Health Records," *IEEE Access*, vol.11, pp.16605–16620, February 2023. https://doi.org/10.1109/access.2023.3245046

[31] M. Hiwale, R. Walambe, V. Potdar, and K. Kotecha, "A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine," *Healthcare Analytics*, vol.3, pp.100192, November 2023. https://doi.org/10.1016/j.health.2023.100192

[32] G. Vukotich, "Healthcare and Cybersecurity: Taking a Zero Trust Approach," *Health Services Insights*, vol. 16, July 2023 https://doi.org/10.1177/11786329231187826

[33] A. Petrosyan, "Statista - The Statistics Portal," Statista. https://www.statista.com/aboutus/our-research-commitment (accessed December 15, 2023).

[34] E. A. Al-Qarni, "Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies," *International Journal of Advanced Computer Science and Applications*, vol.14, no.5, pp.135–140, 2023. https://doi.org/10.14569/ijacsa.2023.0140513

[35] F. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jeréz-Calero, "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare," *Sensors*, vol.23, no.21, pp.1–17, November 2023. https://doi.org/10.3390/s23218944

[36] L. Zhang, Y. Zhu, W. Ren, Y. Zhang, and K. R. Choo, "Privacy-Preserving Fast Three-Factor Authentication and Key Agreement for IoT-Based E-Health Systems," *IEEE Transactions on Services Computing*, vol.16, no.2, pp.1324–1333, February 2022. https://doi.org/10.1109/tsc.2022.3149940

[37] Y. P. Singh, M. A. Jabbar, S. K. Shandilya, O. Вовк, and Y. Hnatiuk, "Exploring applications of blockchain in healthcare: road map and future directions," *Frontiers in Public Health*, vo.11, pp.1–18, September 2023. https://doi.org/10.3389/fpubh.2023.1229386

[38] J. Yang, "Cybersecurity spending in healthcare worldwide 2019-2026," Statista. https://www.statista.com/statistics/1359081/cybersecurity-spending-in-healthcare-sector-worldwide/ (accessed December 9, 2023).

[39] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol.23, no.15, pp.1-20, 2023. https://doi.org/10.3390/s23156666

[40] S. S. Goswami, S. Sarkar, K. C. Gupta, and S. Mondal, "The role of Cyber Security in Advancing Sustainable Digitalization: Opportunities and challenges," *Journal of Decision Analytics and Intelligent Computing*, vol.3, no.1, pp.270–285, 2023. https://doi.org/10.31181/jdaic10018122023g

[41] S. Shitharth and H. Mouratidis, "A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems," *Scientific Reports*, vol.13, no.1, pp.1–21, 2023. https://doi.org/10.1038/s41598-023-34354-x

[42] M. M. Mijwil, M. Aljanabi, and A. H. Ali, "ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information," *Mesopotamian Journal of Cybersecurity*, vol.2023, pp.18–21, 2023. https://doi.org/10.58496/mjcs/2023/004

[43] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," *Cyber Security and Applications*, vol.1, pp.1–13, 2023. https://doi.org/10.1016/j.csa.2023.100016

[44] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Medical 4.0 technologies for healthcare: Features, capabilities, and applications," *Internet of Things and Cyber-Physical Systems*, vol.2, pp.12–30, 2022. https://doi.org/10.1016/j.iotcps.2022.04.001

[45] F. Yan, N. Li, A. M. Iliyasu, A. S. Salama, and K. Hirota, "Insights into security and privacy issues in smart healthcare systems based on medical images," *Journal of Information Security and Applications*, vol.78, pp.1-15, November 2023. https://doi.org/10.1016/j.jisa.2023.103621

[46] Q. Niu, H. Li, L.Yu, Z. Qin, L. Zhang, J. Chen, & Z. Lv, "Toward the Internet of Medical Things: Architecture, trends and challenges," *Mathematical biosciences and engineering*, vol. 21, no. 1, pp. 650–678, Jan. 2023, doi: https://doi.org/10.3934/mbe.2024028.

[47] A. L. Martínez, M. G. Pérez, and A. Ruiz-Martínez, A. "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare," *ACM Computing Surveys*, vol.55, no.12, pp.1–38, 2023. https://doi.org/10.1145/3571156

[48] S. Vermani, "Smart Healthcare: Future Applications & Challenges," *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 15-17 March 2023, pp.131-135.

[49] T. Schroeder, M. Haug, and H. Gewald, "Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study Among Mature Adults," *JMIR formative research*, vol.6, no.6, 1-12, 2022. https://doi.org/10.2196/28025

[50] P. Shojaei, E. Vlahu-Gjorgievska, and Y. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol.13, no.2, pp.1–25, 2024. https://doi.org/10.3390/computers13020041

[51] I. Keshta, and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal*, vol.22, no.2, pp.177–183, 2021. https://doi.org/10.1016/j.eij.2020.07.003

[52] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing Security of Healthcare Data for a Modern Healthcare System," *Sensors*, vol.23, no.7, pp.1–18, March 2023. https://doi.org/10.3390/s23073612

[53] S. Chaudhary, R. Kakkar, K. N. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, D. M. Alshehri, R. Sharma, G. Sharma, and E. I. Davidson, "A Taxonomy on Smart Healthcare Technologies: Security Framework, Case Study, and Future Directions," *Journal of Sensors*, vol.2022, pp.1-30, July 2022. https://doi.org/10.1155/2022/1863838

[54] M. A. Ahmed, H. Sindi, and M. Nour, "Cybersecurity in Hospitals: An Evaluation Model," *Journal of Cybersecurity and Privacy*, vol.2, no.4, pp.853–861, 2022. https://doi.org/10.3390/jcp2040043

[55] A. M. M. Al-Aboosi, S. N. H. S. Abdullah, M. Z. Murah, and G. S. A. Dharhani, "Cybersecurity Trends in Health Information Systems," In 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 06-07 October 2022, pp. 1–4. https://doi.org/10.1109/iccr56254.2022.9995952

[56] K. Konen, L. Cheon, M. Demetriou, M. DePalma, T. Jubran, L. Schleben, F. Nissan, and M. Mahmoud, "Cybersecurity for Modern American Healthcare Institutions," The 2021 World Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, Nevada, USA, 26-29 July 2021, pp.1–10.

[57] A. Majumder and C. B. Veilleux, "Smart Health and Cybersecurity in the Era of Artificial Intelligence. *Computer-Mediated Communication*," IntechOpen, 2021. https://doi.org/10.5772/intechopen.97196

[58] C. V. Herrera, J. Valcárcel, M. Díaz-Reátegui, J. L. H. Salazar, and L. Andrade-Arenas, "Cybersecurity in health sector: a systematic review of the literature," *Indonesian Journal of Electrical Engineering and Computer Science*, vol.31, no.2, pp.1099–1108, 2023. https://doi.org/10.11591/ijeecs.v31.i2.pp1099-1108

[59] A. Ahad, Z. Ali, A. Mateen, M. Tahir, A. Hannan, N. M. García, and I. M. Pires, "A comprehensive review on 5G-based smart healthcare network Security: taxonomy, issues, solutions and future research directions," *Array*, vol.18, pp.1–13, 2023. https://doi.org/10.1016/j.array.2023.100290

[60] A. Dixit, A. Trivedi, and W. W. Godfrey, "A survey of cyber attacks on blockchain based IoT systems for industry 4.0," *IET Blockchain*, pp.1–20, 2022. https://doi.org/10.1049/blc2.12017

[61] R. Talati, and P. Chaudhari, "The Road-ahead for E-healthcare 4.0: A Review of Security Challenges," In 2022 1st International Conference on Informatics (ICI), Noida, India, 14-16 April 2022, pp. 1–6. https://doi.org/10.1109/ici53355.2022.9786917

[62] M. K. Hasan, T. M. Ghazel, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Communications*, vol.16, no.5, pp.421–432, 2022. https://doi.org/10.1049/cmu2.12301

[63] A. B. Haque, B. Bhushan, A. Nawar, K. R. Talha, and S. J. Ayesha, "Attacks and Countermeasures in IoT Based Smart Healthcare Applications," In: Balas V.E., Solanki V.K., Kumar R. (eds) Recent Advances in Internet of Things and Machine Learning. *Intelligent Systems Reference Library*, pp.67–90, 2022. https://doi.org/10.1007/978-3-030-90119-6_6

[64] I. Liu, M. Lee, H. Huang, and J. Li, J. "5G-Based Smart Healthcare and Mobile Network Security: Combating Fake Base Stations," *Applied Sciences*, vol.13, no.20, pp.1–11, 2023. https://doi.org/10.3390/app132011565

[65] N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in iot network using regression modeling," *Advances in Engineering Software*, vol.169, pp.103126, 2022. https://doi.org/10.1016/j.advengsoft.2022.103126

[66] R. Šendelj and I. Ognjanović, "Cybersecurity Challenges in Healthcare," *Studies in Health Technology and Informatics*, vol.300, pp.190–202, 2022. https://doi.org/10.3233/shti220951

[67] R. A. Alsowail and T. Al-Shehari, "Techniques and countermeasures for preventing insider threats," *PeerJ. Computer science*, vol.8, pp.1-37, 2022. https://doi.org/10.7717/peerj-cs.938

[68] Y. Meng, Z. Huang, G. Shen, and C. Ke, "SDN-Based Security Enforcement Framework for Data Sharing Systems of Smart Healthcare," *IEEE Transactions on Network and Service Management*, vol.17, no.1, pp.308–318, 2020. https://doi.org/10.1109/tnsm.2019.2941214

[69] H. Park, P. V. Astillo, Y. Ko, Y. W. Park, T. Kim, and I. You, "SMDFbs: Specification-Based Misbehavior Detection for False Base Stations," *Sensors*, vol.23, no.23, pp.1–15, 2023. https://doi.org/10.3390/s23239504

[70] B. Genge, P. Haller, and A. Roman, "E-APTDetect: Early Advanced Persistent Threat Detection in Critical Infrastructures with Dynamic Attestation," *Applied Sciences*, vol.13, no.6, pp.1–22, 2023. https://doi.org/10.3390/app13063409

[71] M. N. A. Khalid, A. A. Al-Kadhimi, and M. Singh, "Recent Developments in Game-Theory Approaches for the Detection and Defense against Advanced Persistent Threats (APTs): A Systematic Review," *Mathematics*, vol.11, no.6, pp.1–34, 2023. https://doi.org/10.3390/math11061353

[72] T. Jabar, and M. Singh, "Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework," *Sensors*, vol.22, no.13, pp.1–38, 2022. https://doi.org/10.3390/s22134662

[73] Y. Perwej, N. Akhtar, N. Kulshrestha, and P. Mishra, "A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends," *Journal of Emerging Technologies and Innovative Research*, vol.9, no.1, pp.d346–d371, 2022. https://hal.science/hal-03540225

[74] A. A. Al-Kadhimi, M. Singh, and M. N. A. Khalid, "A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques," *Applied Sciences*, vol.13, no. 14, pp. 1–47, 2023. https://doi.org/10.3390/app13148056

[75] M. Waqas, S. Tu, J. Wan, T. Mir, H. Alasmary, and G. Abbas, "Defense scheme against advanced persistent threats in mobile fog computing security," *Computer Networks*, vol.221, pp.109519, 2023. https://doi.org/10.1016/j.comnet.2022.109519

[76] Z. Muhammad, Z. Anwar, A. R. Javed, B. Saleem, S. Abbas, and T. R. Gadekallu, "Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses," *Technologies*, vol.11, no.3, pp.1–50, 2023. https://doi.org/10.3390/technologies11030076

[77] A. Alahmadi, S. U. Rehman, H. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," *Sensors*, vol.22, no.9, pp.1–14, 2022. https://doi.org/10.3390/s22093520

[78] L. Hernández–Álvarez, J. J. B. Pérez, F. K. Batista, and A. Q. Dios, "Security Threats and Cryptographic Protocols for Medical Wearables," *Mathematics*, vol.10, no.6, pp.1–17, 2022. https://doi.org/10.3390/math10060886

[79] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems," *ACM Transactions on Computing for Healthcare*, vol.2, no.3, pp.1–44, 2021. https://doi.org/10.1145/3453176

[80] S. Chaudjary, R. Kakkar, R. Gupta, S. Tanwar, S. Agrawal, and R. V. Sharma, "Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol.30, no.7, pp.2446–2488, 2022. https://doi.org/10.55730/1300-0632.3950

[81] M. Sethi, J. Verma, M. Snehi, V. Baggan, Virender, and G. Chhabra, "Web Server Security Solution for Detecting Cross-site Scripting Attacks in Real-time Using Deep Learning," In 2023 *International Conference on Artificial Intelligence and Applications (ICAIA) Alliance Technology Conference (ATCON-1)*, Bangalore, India, 21-22 April 2023, pp.1–5. https://doi.org/10.1109/icaia57370.2023.10169255

[82] T. Shakeel, S. Habib, W. Boulila, A. Koubâa, A. R. Javed, M. Rizwan, T. R. Gadekallu, and M. Sufiyan, "A survey on COVID-19 impact in the healthcare domain: worldwide market implementation, applications, security and privacy issues, challenges and future prospects," *Complex & Intelligent Systems*, vol.9, no.1, pp.1027–1058, 2023. https://doi.org/10.1007/s40747-022-00767-w

[83] J. Kumar, A. Santhanavijayan, and B. Rajendran, "Cross Site Scripting Attacks Classification using Convolutional Neural Network, " In 2022 *International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 25-27 January 2022, pp.1–6. https://doi.org/10.1109/iccci54379.2022.9740836

[84] M. Indushree, M. Kaur, M. Raj, R. Shashidhara, and H. Lee, "Cross Channel Scripting and Code Injection Attacks on Web and Cloud-Based Applications: A Comprehensive Review," *Sensors*, vol.22, no.5, pp.1–20, 2022. https://doi.org/10.3390/s22051959

[85] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe and A. Welhenge, A. "Security and privacy issues in Medical Internet of Things: Overview, countermeasures, challenges and future directions," *Sustainability*, vol.13, no.21, pp.1–34, 2021. https://doi.org/10.3390/su132111645

[86] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. Singh, and W. Hong, "Internet of Things: Evolution, Concerns and Security Challenges," *Sensors*, vol.21, no.5, pp. 1–33, 2021. https://doi.org/10.3390/s21051809

[87] A. Srhir, T. Mazri, and M. Benbrahim, "Security in the IoT: State-of-the-Art, Issues, Solutions, and Challenges," *International Journal of Advanced Computer Science and Applications*, vol.14, no.5, pp.65–75, 2023. https://doi.org/10.14569/ijacsa.2023.0140507

[88] E. Shaikh, N. Mohammad, A. R. Al-Ali, and S. Muhammad, "A Probabilistic Model Checking (PMC) Approach to Solve Security Issues in Digital Twin (DT)," *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Bengaluru, India, 05-07 January 2023, pp.192–197. https://doi.org/10.1109/idciot56793.2023.10053389

[89] G. Q. Butt, T. A. Sayed, R. Riaz, S. S. Rizvi, and A. Paul, "Secure Healthcare Record Sharing Mechanism with Blockchain," *Applied Sciences*, vol.12, no.5, pp.1–21, 2022. https://doi.org/10.3390/app12052307

[90] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey, "*IEEE Access*, vol.10, pp.93575–93600, 2022. https://doi.org/10.1109/access.2022.3204171

[91] A. Patel, C. Williams, S. N. Hart, C. A. Garcia, T. J. S. Durant, T. C. Cornish, and D. S. McClintock, "Cybersecurity and Information Assurance for the Clinical Laboratory," *The Journal of Applied Laboratory Medicine*, vol.8, no.1, pp.145–161, 2023. https://doi.org/10.1093/jalm/jfac119

[92] M. Wazid, A. K. Das, N. Mohd, and Y. Park, "Healthcare 5.0 security framework: Applications, issues and future research directions," *IEEE Access*, vol.10, pp.129429-129442, December 2022. https://doi.org/10.1109/ACCESS.2022.3228505

[93] M. Zubair, A. Ghubaish, D. Ünal, A. Al-Ali, T. Reimann, G. Alinier, M. Hammoudeh, and Qadir, J. "Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System," *Sensors*, vol.22, no.21, pp.1–23, 2022. https://doi.org/10.3390/s22218280

[94] C. Miller, "3,000 Hospitals Vulnerable Due to Pneumatic Tube Flaws - Information Technology," Healthcare Facilities Today. https://www.healthcarefacilitiestoday.com/posts/3000-Hospitals-Vulnerable-Due-to-Pneumatic-Tube-Flaws--26553 (accessed February 24, 2024)

[95] L. Wasserman, and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," *Frontiers in Digital Health*, vol.4, pp.1–20, 2022. https://doi.org/10.3389/fdgth.2022.862221

[96] A. Kumar, and K. Singh, "Blockchain-Enabled Smart Healthcare Systems Using IoT," in *Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations*, Hampshire: IGI Global, 2023, pp.30–50. https://doi.org/10.4018/978-1-6684-6646-9.ch003

[97] N. Garg, M. Wazid, J. Singh, D. P. Singh, and A. K. Das, "Security in IoMT-driven smart healthcare: A comprehensive review and open challenges," *Security and Privacy*, vol.5, no.5, pp.1–27, 2022. https://doi.org/10.1002/spy2.235

[98] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, A. Alhomoud, A. R. Alharbi, and H. Kumar, "ACM-SH: An Efficient Access Control and Key Establishment Mechanism for Sustainable Smart Healthcare," *Sustainability*, vol.14, no.8, pp.1–17, 2022. https://doi.org/10.3390/su14084661

[99] E. Batista, M. A. Moncusí, P. López-Aguilar, A. Martínez-Ballesté, and A. Solanas, "Sensors for Context-Aware Smart Healthcare: A Security Perspective," *Sensors*, vol.21, no.20, pp.1–60, 2021. https://doi.org/10.3390/s21206886

[100] V. Upadrista, S. Nazir, and H. Tianfield, "Secure data sharing with blockchain for remote health monitoring applications: a review," *Journal of Reliable Intelligent Environments*, vol.9, no.3, pp.349–368, 2023. https://doi.org/10.1007/s40860-023-00204-w

[101] L. Colquhoun. "IoT Security Is Giving Healthcare Heart Attacks." CDOTrends. https://www.cdotrends.com/story/17594/iot-security-giving-healthcare-heart-attacks#:~:text=Cynerio%20researchers%20say%20they%20found,data%20breaches%20involved%20IoT%20devices%E2%80%9D (accessed February 24, 2024).

[102] A. Alabdulatif, I. Khalil, and M. S. Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," *Applied Sciences*, vol.12, no.21, pp.1–32, October 2022. https://doi.org/10.3390/app122111039

[103] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," *Mesopotamian Journal of CyberSecurity*, vol.2023, pp.57–63, March 2023. https://doi.org/10.58496/MJCS/2023/010

[104] M. A. Mohammed, M. Boujelben, and M. Abid, "A Novel Approach for Fraud Detection in Blockchain-Based Healthcare Networks Using Machine Learning," *Future Internet*, vol.15, no.8, pp.1–18, 2023. https://doi.org/10.3390/fi15080250

[105] V. Pandagle, "Legacy Systems In Healthcare Impact Growth, Data Security." The Cyber Express. https://thecyberexpress.com/legacy-systems-in-healthcare-hinder-growth/ (accessed February 13, 2024).

[106] S. Renukappa, P. Mudiyia, S. Suresh, W. Abdalla, and C. Subbarao, "Evaluation of challenges for adoption of smart healthcare strategies," *Smart Health*, vol.26, pp.1–14, 2022. https://doi.org/10.1016/j.smhl.2022.100330

[107] A. Aljaloud, and A. Razzaq, "Modernizing the Legacy Healthcare System to Decentralize Platform Using Blockchain Technology," *Technologies*, vol.11, no.4, pp.1–17, 2023. https://doi.org/10.3390/technologies11040084

[108] S. Islam, S. Papastergiou, E. Kalogeraki, and K. Kioskli, "Cyberattack Path Generation and Prioritisation for Securing Healthcare Systems," *Applied Sciences*, vol.12, no.9, pp.1–22, 2022. https://doi.org/10.3390/app12094443

[109] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions," *IEEE Communications Surveys and Tutorials*, vol.25, no.1, pp.386–424, 2023. https://doi.org/10.1109/comst.2022.3224644

[110] X. Zhang, M. Pike, N. Mustafa, and V. Brusic, "Ethically Informed Software Process for Smart Health Home," *2022 IEEE 35th International Symposium on Computer-Based Medical Systems (CBMS)*, Shenzen, China, 21-23 July 2022, pp.187–192. https://doi.org/10.1109/cbms55023.2022.00040

[111] M. M. Akhtar, A. Haleem, and M. Javaid, "Scope of health care system in rural areas under Medical 4.0 environment," *Intelligent Pharmacy*, vol.1, no.4, pp.217–223, 2023. https://doi.org/10.1016/j.ipha.2023.07.003

[112] D. Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," *Healthcare*, vol.11, no.6, pp.1–24, 2023. https://doi.org/10.3390/healthcare11060911

[113] H. Lin, K. Kaur, X. Wang, G. Kaddoum, J. Hu, and M. M. Hassan,"Privacy-Aware Access Control in IoT-Enabled Healthcare: A Federated Deep Learning Approach," *IEEE Internet of Things Journal*, vol.10, no.4, pp.2893–2902, 2023. https://doi.org/10.1109/jiot.2021.3112686

[114] P. Twenter, "2 in 3 healthcare organizations' supply chains attacked: Report." Becker's Hospital Review. https://www.beckershospitalreview.com/supply-chain/2-in-3-healthcare-organizations-supply-chains-attacked-report.html (accessed February 16, 2024).

[115] A. Wilner, H. Luce, E. Ouellet, O. Williams, and N. Costa, "From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector," *International Journal*, vol.76, no.4, pp.522–543, 2022. https://doi.org/10.1177/00207020211067946

[116] S. J. Kirubakaran, A. Gunasekaran, D. R. J. Dolly, D. J. Jagannath, and J. D. Peter, "A feasible approach to smart remote health monitoring: Subscription-based model," *Frontiers in public health*, vol.11, pp.1-6, 2023. https://doi.org/10.3389/fpubh.2023.1150455

[117] H. A. Noman, O. M. F. Abu-Sharkh, "Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations," *Sensors*, vol.23, no.13, pp.1–53, 2023. https://doi.org/10.3390/s23136067

[118] V. Abdullayev and A. S. Chauhan, "SQL Injection Attack: Quick View," *Mesopotamian Journal of Cybersecurity*, vol.2023, pp.30–34, 2023. https://doi.org/10.58496/mjcs/2023/006

[119] M. Alghawazi, D. Alghazzawi, S. Alarifi, S. "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review," *Journal of Cybersecurity and Privacy*, vol.2, no.4, pp.764–777, 2022. https://doi.org/10.3390/jcp2040039

[120] R. Veluvarthi, A. Rameswarapu, K. V. Kalyan, J. Piri, and B. Acharya, "Security and Privacy Threats of IoT Devices: A & Short Review," In 2023 *4th International Conference on Signal Processing and Communication (ICSPC)*, Coimbatore, India, 23-24 March 2023, pp.32–37. https://doi.org/10.1109/icspc57692.2023.10125863

[121] K. Karunanithy, and V. Bhanumathi, "Edge device based efficient data collection in smart health monitoring system using wireless body area network," *Biomedical Signal Processing and Control*, vol.72, pp.103280, 2022. https://doi.org/10.1016/j.bspc.2021.103280

[122] H. Verma, N. Chauhan, N. Chand, and L. K. Awasthi, "Buffer-loss estimation to address congestion in 6LoWPAN based resource-restricted 'Internet of Healthcare Things' network," *Computer Communications*, vol.181, pp.236–256, 2022. https://doi.org/10.1016/j.comcom.2021.10.016

[123] A. Sheikh, S. Kumar, and A. Ambhaikar, "An Energy-Efficient Approach for the Security of IoT Networks using SCEER," In 2022 *1st International Conference on Informatics (ICI)*, Noida, India, 14-16 April 2022, pp.1–6. https://doi.org/10.1109/ici53355.2022.9786919

[124] A. Albattah and M. A. Rassam, "Detection of Adversarial Attacks against the Hybrid Convolutional Long Short-Term Memory Deep Learning Technique for Healthcare Monitoring Applications," *Applied Sciences*, vol.13, no.11, pp.1–17, 2023. https://doi.org/10.3390/app13116807

[125] K. A. Ali, and S. Alyounis, "CyberSecurity in Healthcare Industry," *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, 14-15 July 2021, pp. 695-701. https://doi.org/10.1109/icit52682.2021.9491669

[126] A. A. Sharah, H. A. Owida, T. A. Edwan, and F. Alnaimat, "A Cooperative Smart Jamming Attack in Internet of Things Networks," *Journal of Information and Communication Convergence Engineering*, vol.20, no.4, pp.250–258, 2022. https://doi.org/10.56977/jicce.2022.20.4.250

[127] G. Sharma, and G. Singh, “Robust User Authentication Scheme for IoT-Based Healthcare Applications,” *Advances in Medical Technologies and Clinical Practice Book Series*, IGI Global, 2023, pp.170–182. https://doi.org/10.4018/978-1-6684-6434-2.ch008

[128] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, “Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications,” *Sustainability*, vol.14, no.23, pp.1–15, 2022. https://doi.org/10.3390/su142315900

[129] K. R. Saraf and P. Malathi, “Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare,” *International Journal of Intelligent Systems and Applications in Engineering*, vol.11, no.2, pp.537–549, 2023. https://ijisae.org/index.php/IJISAE/article/view/2709

[130] R. Qureshi, M. Asad, S. Tunio, S. Qureshi, M. Ahmed, M. and A. Ghulam, "A Survey on Security Issues and Attacks of Fog Computing," *VFAST Transactions on Software Engineering*, vol.11, no.1, pp.1–11, 2023. https://doi.org/10.21015/vtse.v11i1.1309

[131] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K. R. Choo, ”Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies,” *IEEE Internet of Things Journal*, vol.9, no.1, pp.199–221, 2022. https://doi.org/10.1109/jiot.2021.3079916

[132] K. Rajkumar and U. Hariharan, "Analytics for data security and privacy in 5G health-care services," in *Blockchain for 5G Healthcare Applications: Security and Privacy Solutions*, IET Digital Library, 2021, pp. 315–345. https://doi.org/10.1049/pbhe035e_ch12

[133] M. Hassan, N. Tariq, A. Alsirhani, A. Alomari, F. A. Khan, M. M. Alshahrani, M. Ashraf, and M. Humayun, “GITM: A GINI Index-Based Trust Mechanism to Mitigate and Isolate Sybil Attack in RPL-Enabled Smart Grid Advanced Metering Infrastructures,” *IEEE Access*, vol.11, pp.62697–62720, 2023. https://doi.org/10.1109/access.2023.3286536

[134] A. Shaji and N. S. Nair, “A Novel Trust Based Two Phase Algorithm to Detect Sybil Attack in IoMT Networks,” *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, Kochi, Kerala, India, 17-19 August 2023, pp.309–314. https://doi.org/10.1109/icscc59169.2023.10334946

[135] A. S. S. Thuluva, M. S. Somanathan, S. Ramasubbareddy, S. Sennan, and D. Burgos, “Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT,” *EURASIP Journal on Advances in Signal Processing*, vol.2021, no.1, pp.1–23, 2021. https://doi.org/10.1186/s13634-021-00748-0

[136] S. E. Ali, N. Tariq, F. A. Khan, M. Ashraf, W. Abdul, and K. Saleem, “BFT-IoMT: A Blockchain-Based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things,” *Sensors*, vol.23, no.9, pp.1–17, 2023. https://doi.org/10.3390/s23094265

[137] D. Arshad, M. Asim, N. Tariq, T. Baker, H. Tawfik, and D. Al-Jumeily, “THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack,” *PLoS ONE*, vol.17, no.7, pp.1–33, 2022. https://doi.org/10.1371/journal.pone.0271277

[138] A. A. Khan, A. Ahmad, M. Waseem, P. Liang, M. Fahmideh, T. Mikkonen, and P. Abrahamsson, “Software architecture for quantum computing systems — A systematic review,” *Journal of Systems and Software*, vol.201, pp.1–29, 2023. https://doi.org/10.1016/j.jss.2023.111682

[139] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, ”Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions,” *Information Fusion*, vol.102, pp.1–20, 2024. https://doi.org/10.1016/j.inffus.2023.102060

[140] A. Arafa, H. Sheerah, and S. Alsalamah, “Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review,” *Information*, vol.14, no.12, pp.1–15, 2023. https://doi.org/10.3390/info14120640

[141] B. S. Shukur, M. Aljanabi, and A. H. Ali, “ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information,” *Mesopotamian Journal of Cybersecurity*, pp.18–21, 2023. https://doi.org/10.58496/mjcs/2023/004

[142] H. Szczepaniuk and E. K. Szczepaniuk, “Cryptographic evidence-based cybersecurity for smart healthcare systems,” *Information Sciences*, vol.649, pp.1–23, 2023. https://doi.org/10.1016/j.ins.2023.119633

[143] D. Said, “Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid,” *Energies*, vol.16, no.8, pp.1–11, 2023. https://doi.org/10.3390/en16083572

[144] V. K. Pallaw, K. U. Singh, A. Kumar, T. Singh, C. Swarup, and A. Goswami, “A Robust Medical Image Watermarking Scheme Based on Nature-Inspired Optimization for Telemedicine Applications,” *Electronics*, vol.12, no.2, pp.1–18, 2023. https://doi.org/10.3390/electronics12020334

[145] D. Awasthi, P. Khare, and V. K. Srivastava, “BacterialWmark: telemedicine watermarking technique using bacterial foraging for smart healthcare system,” *Journal of Electronic Imaging*, vol.32, no.04, pp.042107-1-042107–042115, 2023. https://doi.org/10.1117/1.jei.32.4.042107

[146] S. Gull and S. A. Parah, “Advances in medical image watermarking: a state of the art review,” *Multimedia Tools and Applications*, vol.83, no.1, pp.1407–1447, 2024. https://doi.org/10.1007/s11042-023-15396-9

[147] E. A. Hachim and Y. M. Mohialden, “Cloud-based digital watermarking model for medical image integrity,” *Scientific Research Journal of Engineering and Computer Science*, vol.3, no.5, pp.1-6, 2023.

[148] M. Sajeer and A. Mishra, “A robust and secured fusion based hybrid medical image watermarking approach using RDWT-DWT-MSVD with Hyperchaotic system-Fibonacci Q Matrix encryption,” *Multimedia tools and applications*, pp.1–23, 2023. Advance online publication. https://doi.org/10.1007/s11042-023-15001-z

[149] B. Abd-El-Atty, “A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks,” *Neural Computing and Applications*, vol.35, no.1, pp.773–785, 2023. https://doi.org/10.1007/s00521-022-07830-0

[150] H. N. AlEisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things," *Journal of Healthcare Engineering*, vol.2022, pp.1–11, 2022. https://doi.org/10.1155/2022/7528583

[151] B. R. Louassef, and N. Chikouche, "Privacy preservation in healthcare systems," *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*, El Oued, Algeria, 20-21 November 2021, pp. 1–6. https://doi.org/10.1109/ai-csp52968.2021.9671083

[152] B. Kumar, "Patient-Controlled Mechanism Using Pseudonymization Technique for Ensuring the Security and Privacy of Electronic Health Records," *International Journal of Reliable and Quality E-healthcare*, vol.11, no.1, pp.1–15, 2022. https://doi.org/10.4018/ijrqeh.297076

[153] Z. Jamroz, I. Ullah, B. Hassan, N. U. Amin, M. A. Khan, P. Lorenz, and N. Innab, "An Optimal Authentication Scheme through Dual Signature for the Internet of Medical Things," *Future Internet*, vol.15, no.8, pp.1–14, 2023. https://doi.org/10.3390/fi15080258

[154] S. Rani, A. Kataria, S. Kumar, and P. Tiwari, "Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review," *Knowledge-Based Systems*, vol.274, pp.1–28, 2023. https://doi.org/10.1016/j.knosys.2023.110658

[155] J. Andrew, J. Karthikeyan, J. Eunice, M. Pomplun, and H. Dang, "Privacy Preserving Attribute-Focused Anonymization Scheme for Healthcare Data Publishing," *IEEE Access*, vol.10, pp.86979–86997, 2022. https://doi.org/10.1109/access.2022.3199433

[156] F. Mosaiyebzadeh, S. Pouriyeh, R. M. Parizi, Q. Z. Sheng, M. Han, L. Zhao, G. Sannino, C. M. Ranieri, J. Ueyama, and D. M. Batista, "Privacy-Enhancing Technologies in Federated Learning for the Internet of Healthcare Things: A Survey," *Electronics*, vol.12 no.12, pp.1–28, 2023. https://doi.org/10.3390/electronics12122703

[157] D. E. Majdoubi, H. E. Bakkali, S. Sadki, Z. Maqour, and A. Leghmid, "The Systematic Literature Review of Privacy-Preserving Solutions in Smart Healthcare Environment," *Security and Communication Networks*, vol.2022, pp.1–26, 2022. https://doi.org/10.1155/2022/5642026

[158] K. Sowjanya, M. Dasgupta, and S. Ray, "A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems," *Journal of Systems Architecture*, vol.117, pp.102108, 2021. https://doi.org/10.1016/j.sysarc.2021.102108

[159] R. R. T. Da Silva, N. Antunes, and A. H. F. De Morais, "Privacy in electronic health records: a systematic mapping study," *Journal of Public Health*, pp.1–20, 2024. https://doi.org/10.1007/s10389-022-01795-z

[160] A. Alzu'bi, A. Alomar, S. Alkhaza'leh, A. Abuarqoub, and M. Hammoudeh, "A Review of Privacy and Security of Edge Computing in Smart Healthcare Systems: Issues, Challenges, and Research Directions," *Tsinghua Science & Technology*, vol.29 no.4, pp.1152–1180, 2024. https://doi.org/10.26599/tst.2023.9010080

[161] P. Nag, P. Chandrakar, and K. Chandrakar, "An Improved Two-Factor Authentication Scheme for Healthcare System," *Procedia Computer Science*, vol.218, pp.1079–1090, 2023. https://doi.org/10.1016/j.procs.2023.01.087

[162] S. Das, S. Namasudra, S. Deb, P. Moreno-Ger, and R. G. Crespo, "Securing IoT-Based Smart Healthcare Systems by Using Advanced Lightweight Privacy-Preserving Authentication Scheme," *IEEE Internet of Things Journal*, vol.10 no.21, pp.18486–18494, 2023. https://doi.org/10.1109/jiot.2023.3283347

[163] K. Thilagam, A. Beno, M. P. Lakshmi, C. B. Wilfred, S. M. George, M. Karthikeyan, P. Vijayakumar, C. Ramesh, and P. Karunakaran, "Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System," *Journal of Nanomaterials*, vol.2022, pp.1–8, 2022. https://doi.org/10.1155/2022/2638613

[164] T. Suleski, M. Ahmed, W. Yang, and E. Wang, "A review of multi-factor authentication in the Internet of Healthcare Things," *Digital Health*, vol.9, pp.1–20, 2023. https://doi.org/10.1177/20552076231177144

[165] S. Monga and D. Singh, "MRBSChain a novel scalable medical records binance smart chain framework enabling a paradigm shift in medical records management," *Scientific Reports*, vol.12 no.1, pp.1–12, 2022. https://doi.org/10.1038/s41598-022-22569-3

[166] T. A. Alhaj, S. M. Abdulla, M. a. E. Iderss, A. a. A. Ali, F. A. Elhaj, M. A. Remli, and L. A. Gabralla, "A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT)," *IEEE Access*, vol.10, pp.124777–124791, 2022. https://doi.org/10.1109/access.2022.3225038

[167] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," *IEEE Access*, vol.11, pp.145869–145896, 2023. https://doi.org/10.1109/access.2023.3346320

[168] K. Vilakazi, and F. Adebesin, "A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies," *Proceedings of Society 5.0 Conference 2023*, vol.93, pp. 240–251. https://doi.org/10.29007/hf15

[169] C. Stergiou, A. P. Plageras, V. A. Memos, M. P. Koidou, and K. E. Psannis, "Secure Monitoring System for IoT Healthcare Data in the Cloud," *Applied Sciences*, vol.14 no.1, pp.1–16, 2024. https://doi.org/10.3390/app14010120

[170] R. W. Mponda, K. M. A. Sithik, and Tawarish, "Smart Health System and Electronic Health Passport," *International Journal of Research Publication and Reviews*, vol.5, no.2, pp.3197–3201, 2024. https://ijrpr.com/uploads/V5ISSUE2/IJRPR22940.pdf

[171] R. Marshal, K. Gobinath, and V. V. Rao, "Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks," *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Toronto, ON, Canada, 21-24 April 2021, pp.1–4. https://doi.org/10.1109/iemtronics52119.2021.9422615

[172] N. Dissanayake, M. Zahedi, A. Jayatilaka, and M. A. Babar, "Why, How and Where of Delays in Software Security Patch Management: An Empirical Investigation in the Healthcare Sector," *Proceedings of the ACM on Human-*

Computer Interaction, vol.6, No.CSCW2, New York, NY, United States, November 2022, pp.1–29. https://doi.org/10.1145/3555087

[173] V. Agrawal, S. Agrawal, A. Bomanwar, T. Dubey, and A. Jaiswal, "Exploring the Risks, Benefits, Advances, and Challenges in Internet Integration in Medicine With the Advent of 5G Technology: A Comprehensive Review," *Cureus*, vol.15, no.11, pp.1-16, 2023. https://doi.org/10.7759/cureus.48767

[174] S. Abdulmalek, A. Nasir, and W. A. Jabbar, "LoRaWAN-based Hybrid Internet of Wearable Things System Implementation for Smart Healthcare," *Internet of Things*, vol.25, pp.1–21, 2024. https://doi.org/10.1016/j.iot.2024.101124

[175] J. Kongsen, D. Chantaradsuwan, P. Koad, M. Thu, and C. Jandaeng, "A Secure Blockchain-Enabled Remote Healthcare Monitoring System for Home Isolation," *Journal of Sensor and Actuator Networks*, vol.13, no.1, pp.1–20, 2024. https://doi.org/10.3390/jsan13010013

[176] C. Li, J. Wang, S. Wang, and Y. Zhang, "A Review of IoT Applications in Healthcare," *Neurocomputing*, vol.565, pp.1–12, 2024. https://doi.org/10.1016/j.neucom.2023.127017

[177] A. M. Said, A. Yahyaoui, and T. Abdellatif, "Efficient Anomaly Detection for Smart Hospital IoT Systems," *Sensors*, vol.21, no.4, pp.1–24, 2021. https://doi.org/10.3390/s21041026

[178] A. Baz, R. Ahmed, S. R. Khan, and S. Kumar, "Security Risk Assessment Framework for the Healthcare Industry 5.0," *Sustainability*, vol.15, no.23, pp.1–27, 2023. https://doi.org/10.3390/su152316519

[179] S. Ksibi, F. Jaïdi, and A. Bouhoula, "A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach," *Mobile Networks and Applications*, vol.28, no.1, pp.107–127, 2022. https://doi.org/10.1007/s11036-022-02042-1

[180] Pritika, B. Shanmugam, and S. Azam, "Risk Assessment of Heterogeneous IoMT Devices: A Review," *Technologies*, vol.11, no.1, pp.1–34, 2023. https://doi.org/10.3390/technologies11010031

[181] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, "Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal," *IEEE Access*, vol.9, pp.40049–40075, 2021. https://doi.org/10.1109/access.2021.3064682

[182] A. Yadav, N. Ahmad, I. R. Khan, P. Agarwal, and H. Kaur, "Role of AI, Big data in Smart Healthcare System," *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, 03-04 March 2023, pp.1–8. https://doi.org/10.1109/iscon57294.2023.10111971

[183] M. Al-Hawawreh, N. Moustafa, and J. Slay, "A threat intelligence framework for protecting smart satellite-based healthcare networks, "*Neural Computing and Applications*, vol.36, no.1, pp.15–35, 2024. https://doi.org/10.1007/s00521-021-06441-5

[184] W. Zhang, Y. Bai, and J. Feng, "TIIA: A blockchain-enabled Threat Intelligence Integrity Audit scheme for IioT," *Future Generation Computer Systems*, vol.132, pp.254–265, 2022. https://doi.org/10.1016/j.future.2022.02.023

[185] H. Ali, J. Ahmad, Z. Jaroucheh, P. Papadopoulos, N. Pitropakis, O. Lo, W. Abramson, and W. J. Buchanan, "Trusted Threat Intelligence Sharing in Practice and Performance Benchmarking through the Hyperledger Fabric Platform," *Entropy*, vol.24, no.10, pp.1-32, 2022. https://doi.org/10.3390/e24101379

[186] W. Maina, L. Nderu, and T. Mwalili, "A Smart Contract Approach to Cyber Threat Intelligence Sharing in Kenya," *2022 IST-Africa Conference (IST-Africa)*, Ireland, 16-20 May 2022, pp.1–10. https://doi.org/10.23919/ist-africa56635.2022.9845603

[187] J. V. B. Benifa, G. V. Mini, and S. Krishnan, "Blockchain-based health care monitoring for privacy preservation of COVID-19 medical records," in *Blockchain for Smart Cities*, ScienceDirect, 2021, pp.259–294. https://doi.org/10.1016/b978-0-12-824446-3.00005-3

[188] L. Wang, X. Liu, W. Shao, C. Y. Guan, Q. Huang, S. Xu, and S. Zhang, "A Blockchain-Based Privacy-Preserving Healthcare Data Sharing Scheme for Incremental Updates," *Symmetry*, vol.16, no.1, pp.1–17, 2024. https://doi.org/10.3390/sym16010089

[189] I. Bala, M. M. Mijwil, G. Ali, and E. Sadıkoğlu, "Analysing the Connection Between AI and Industry 4.0 from a Cybersecurity Perspective: Defending the Smart Revolution," *Mesopotamian Journal of Big Data*, vol.2023, pp.63–69, 2023. https://doi.org/10.58496/mjbd/2023/009

[190] A. H. Omran, S. Mohammed, and M. Aljanabi, "Detecting Data Poisoning Attacks in Federated Learning for Healthcare Applications Using Deep Learning," *Iraqi Journal for Computer Science and Mathematics*, vol.4, no.4, pp.225–237, 2023. https://doi.org/10.52866/ijcsm.2023.04.04.018

[191] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," *Scientific Reports*, vol.14, no.1, pp.1–16, 2024. https://doi.org/10.1038/s41598-024-56126-x

[192] A. M. Judith, G. J. W. Kathrine, S. Silas, and J. Andrew, "Efficient Deep Learning-Based Cyber-Attack Detection for Internet of Medical Things Devices," *Engineering Proceedings*, vol.59, no.1, pp.1–10, 2023. https://doi.org/10.3390/engproc2023059139

[193] E. C. P. Neto, S. Dadkhah, S. Sadeghi, H. Molyneaux, and A. A. Ghorbani, "A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective," *Computer Communications*, vol.213, pp.61–77, 2024. https://doi.org/10.1016/j.comcom.2023.11.002

[194] A. V. L. N. Sujith, G. S. Sajja, V. Mahalakshmi, S. Nuhmani, and P. Balaji, "Systematic review of smart health monitoring using deep learning and Artificial intelligence," *Neuroscience Informatics*, vol.2, no.3, pp.1–6, 2022. https://doi.org/10.1016/j.neuri.2021.100028

[195] Y. Chen, L. Zhang, and M. Wei, "How Does Smart Healthcare Service Affect Resident Health in the Digital Age? Empirical Evidence From 105 Cities of China, *Frontiers in Public Health*, vol.9, pp.1–10, 2022. https://doi.org/10.3389/fpubh.2021.833687

[196] D. Tin, R. Hata, F. Granholm, R. G. Ciottone, R. Staynings, and G. R. Ciottone, "Cyberthreats: A primer for healthcare professionals," *The American Journal of Emergency Medicine*, vol.68, pp.179–185, 2023. https://doi.org/10.1016/j.ajem.2023.04.001

[197] M. P. Carello, A. Marchetti-Spaccamela, L. Querzoni, and M. Angelini, "SoK: Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector.," *2023 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Charlotte, NC, USA, 02-03 October 2023, pp. 1–6. https://doi.org/10.1109/isi58743.2023.10297246

[198] G. Mishra, "A Comprehensive Review of Smart Healthcare Systems: Architecture, Applications, Challenges, and Future Directions," *International Journal of Innovative Research in Technology and Science*, vol.12, no.2, pp.210-218, 2024. https://ijirts.org/index.php/ijirts/article/view/32

[199] A. Husnain, S. N. Rasool, A. Saeed, A. Y. Gill, and H. K. Hussain, "AI's Healing Touch: Examining Machine Learning's Transformative Effects on Healthcare," *Journal of World Science*, vol.2, no.10, pp.1681–1695, 2023. https://doi.org/10.58344/jws.v2i10.448

[200] G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, "A Comprehensive Review of Cyber Threats and Attacks, and Mitigation Techniques in FinTech," *Iraqi Journal for Computer Science and Mathematics*, vol.5, no.3, In press, 2024.