applied sciences

MDPI

Review

A Comprehensive Survey of Cybersecurity Thraat s and Data Privacy Issues in Healthcare Systems

Ramsha Qureshi and Insoo Koo *

Department of Electrical Electronic and Computer Engineering, University of Ulsan, Ulsan 44610, Republic of Korea; ramsha46@mail.ulsan.ac.kr
* Correspondence: iskoo@ulsan.ac.kr

Abstract

The rapid digital transformation of healthcare has improved clinical efficiency, patient engagement, and data accessibility, but it has also introduced significant cyber security and data privacy challenges. Healthcare IT systems increasingly rely on interconnected networks, electronic health records (EHRs), tele-medicine platforms, cloud infrastructures, and Internet of Medical Things (IoMT) devices, which collectively expand the attack surface for cyber threats. This scoping review maps and synthesizes recent evidence on cyber security risks in healthcare, including ransomware, data breaches, insider threats, and vulnerabilities in legacy systems, and examines key data privacy concerns related to patient confidentiality, regulatory compliance, and secure data governance. We also review contemporary security strategies, including encryption, multi-factor authentication, zero-trust architecture, blockchain-based approaches, AI-enabled threat detcetion and compliance frameworks such as HIPAA and GDPR. Persistent challenges include integrating robust security with clinical usability, protecting resource-limited hospital environments, and managing human factors such as staff awareness and policy adherence. Overall, the findings suggest that effective healthcare cyber security requires a multi-layered defense combining technical controls, continuous monitoring, governance and regulatory alignment, and sustained organizational commitment to security culture. Future research should prioritize adaptive security models, improved standardization, and privacy-preserving analytics to protect patient data in increasingly complex healthcare ecosystems.

Keywords: cybersecurity in healthcare; security attacks on healthcare systems; data privacy in healthcare; blockchain; electronic health record security; e-healthcare; patient monitoring; Internet of Medical Things; IoMT

Academic Editor: Gianluca Lax

Received: 21 December 2025
Revised: 27 January 2026
Accepted: 28 January 2026
Published: 2 February 2026

1. Introduction

The digital transformation of healthcare has driven the widespread adoption of interconnected information technologies, including electronic health records (EHRs) [1], telemedicine platforms, cloud-based services, mobile health applications, and Internet of Medical Things (IoMT) devices. These technologies have substantially enhanced healthcare delivery by enabling faster diagnosis, improved data accessibility, and more coordinated patient care. However, the growing dependence on such digital infrastructures has also significantly increased the exposure of healthcare organizations to sophisticated cybersecurity threats and data privacy risks.

Healthcare data is particularly attractive to cybercriminals because it contains sensitive personal information, financial records, and medical histories that can be exploited for iden-

tity theft, insurance fraud, or unauthorized resale [2]. Cyberattacks such as ransomware, phishing, data breaches, and IoT-based intrusions have surged globally, disrupting clinical operations, threatening patient safety, and damaging the integrity and availability of healthcare systems. As healthcare environments expand in scale and complexity, legacy software, insufficient network security, weak authentication practices, and limited staff awareness further amplify the probability of successful attacks.

In response, healthcare institutions are adopting stronger cybersecurity and data protection frameworks that combine technological, procedural, and regulatory strategies [3]. Technical solutions include encryption, multifactor authentication, secure network segmentation, intrusion detection systems, AI-based threat monitoring, blockchain-based data integrity mechanisms, and zero-trust architecture. At the same time, legal and regulatory frameworks such as HIPAA, GDPR, and national healthcare security policies mandate strict requirements for secure data access [4], storage, and governance. Organizational strategies such as risk assessment, incident response planning, continuous monitoring, and cybersecurity awareness training also play a critical role in strengthening resilience [5].

Figure 1 depicts an interconnected healthcare ecosystem built around Internet of Medical Things (IoMT) technologies, where patients, healthcare professionals, edge devices, and cloud services interact to support continuous care delivery. Wearable and implantable medical devices collect real-time physiological data from patients and transmit them through local edge nodes to healthcare assistants and clinicians for monitoring and clinical assessment. Medical staff, including nurses, doctors, and IT management personnel, access this information through secure healthcare systems to enable remote consultation, decision support, and data management. Supporting components such as medical drones and smart ambulances extend this ecosystem by facilitating remote sample collection and emergency response, while the presence of threat actors highlights the need for robust security controls.

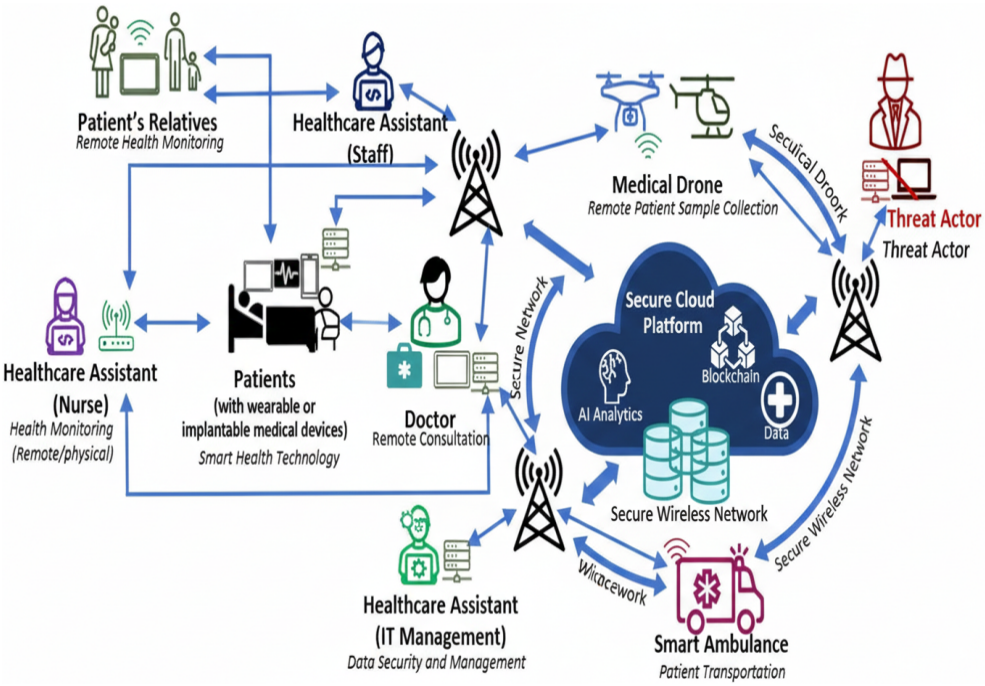

Figure 1. Architecture of the healthcare systems.

Communication between edge devices, healthcare systems, and cloud services is secured using modern transport-layer protection mechanisms, specifically TLS 1.3 with strong cipher suites such as AES-256-GCM or ChaCha20-Poly1305, to safeguard data during transmission. Cryptographic key management is handled through centralized key-management

https://doi.org/10.3390/app16031511

services or hardware security modules, enabling secure key generation, storage, rotation, and revocation. Data stored within the cloud infrastructure is protected using symmetric encryption, while access to resources is governed by certificate-based identity management and role-based access control policies. Together, these measures ensure confidentiality, integrity, and controlled access across the ecosystem, thereby realizing the "secure" property highlighted in the cloud platform component of the architecture.

Despite significant progress, major challenges remain. Many healthcare organizations struggle with limited security budgets, fragmented systems, inconsistent compliance enforcement [6], and the difficulties of maintaining strong defenses in rapidly evolving digital environments. As cyber threats become more adaptive and automated, the need for robust, scalable, and intelligent security solutions is greater than ever. Therefore, developing effective cybersecurity and data privacy strategies is essential not only for regulatory compliance but also for safeguarding patient trust, ensuring continuity of care, and preserving the stability of modern healthcare IT systems.

The rapid digitization of healthcare has transformed clinical operations, patient management, and medical data processing [7], but has also significantly increased the cybersecurity risks faced by healthcare organizations. As healthcare systems integrate electronic health records (EHRs), cloud platforms, telemedicine, connected medical devices, and Internet of Medical Things (IoMT) technologies, new vulnerabilities emerge that expand the attack surface for cybercriminals, making healthcare one of the most targeted sectors today. Cybercrime in healthcare has grown steadily due to inherent weaknesses in digital infrastructures, including vulnerabilities in hardware, software, operating systems, and human processes, all of which can be exploited to disrupt services or compromise sensitive health information [8]. Recent cybersecurity incidents highlight the severity and consequences of breaches in healthcare environments. Attacks such as ransomware, phishing, malware infiltration, and insider misuse can lead to operational shutdowns, manipulation of clinical data, financial loss, and violations of patient confidentiality. Healthcare institutions have experienced increasingly sophisticated cyberattacks that damage system integrity, delay treatments, hinder business operations, and expose sensitive patient data for financial gain or malicious exploitation [7]. With incidents such as the Universal Health Services ransomware attack and large-scale breaches like SingHealth, it has become clear that cyber threats now represent major operational and regulatory challenges for healthcare systems across the world.

To respond to emerging cyber threats, healthcare organizations need to adopt advanced defensive strategies, including artificial intelligence-based threat detection, zero-trust architecture (ZTA), blockchain-based data integrity solutions, and improved workforce training to mitigate human-driven risks [9]. At the same time, academic research continues to emphasize the need for comprehensive, multi-layered cybersecurity approaches that address not only technology, but also organizational culture, risk management, and proactive prevention. As cyberattacks evolve in frequency and complexity, strengthening cybersecurity and data privacy has become essential for maintaining system resilience, protecting patient information, and preserving the trust and functionality of modern healthcare IT systems [10].

The rapid integration of Internet of Things (IoT) technologies into healthcare systems has fundamentally transformed medical services by enhancing patient monitoring, diagnostic accuracy, and personalized care delivery. However, this increased connectivity has simultaneously introduced significant cybersecurity vulnerabilities, posing threats to the confidentiality, safety, and reliability of healthcare information systems [11]. As healthcare IoT ecosystems continue to expand in scale and complexity, they present an enlarged attack

surface that can be exploited by cyber adversaries targeting medical devices, communication networks, and system configurations [12].

Cyber threats in healthcare IoT systems pose a direct danger not only to digital assets but also to patient well-being, as compromised devices can disrupt treatments or manipulate clinical data. Traditional threat analysis and security evaluation methods have become insufficient in addressing this evolving landscape, especially when attackers use dynamic and adaptive intrusion strategies. Therefore, healthcare systems require more intelligent and flexible defense mechanisms capable of learning from changing threat behaviors [13].

2. Background and Motivation

The digitization of healthcare has introduced modern information systems and connected medical devices that support clinical workflows, electronic health records, remote monitoring, smart diagnostics, and automated care delivery. These developments have transformed healthcare into a highly interconnected computational environment where patient data is continuously exchanged across devices, networks, and applications [14]. However, this rapid expansion has also widened the security perimeter and increased the number of attack vectors that cyber adversaries can exploit.

The emergence of the Internet of Medical Things (IoMT) has significantly accelerated this transformation by enabling medical sensors, infusion pumps, imaging devices, and monitoring systems to operate autonomously and communicate digitally within healthcare networks [15]. While this supports faster clinical decision-making and improved operational efficiency, the diversification of devices and growing systemic interdependencies also introduces numerous vulnerabilities in firmware, device communication pathways, network links, and application software.

Healthcare systems also face significant operational pressures, including rising patient data volumes, the need for continuous system availability, and reliance on real-time digital access. In such environments, cyber incidents can directly jeopardize patient outcomes by disrupting clinical workflows or altering medical device behavior [16]. Consequently, cybersecurity and data protection have become critical challenges in maintaining the integrity, safety, and availability of modern healthcare IT systems.

3. Research Methodology

3.1. Methodology Scope and Review Framework

This study adopts a *scoping review* (systematic mapping) methodology guided by the PRISMA-ScR reporting framework to examine cybersecurity threats and data privacy issues in healthcare systems. A scoping review is appropriate for this topic because the evidence base is broad and heterogeneous, spanning technical, organizational, and regulatory dimensions. The objective is to transparently identify, screen, and map relevant literature, and to synthesize findings thematically rather than perform quantitative meta-analysis.

The scope of the review covers cybersecurity threats, privacy vulnerabilities, regulatory considerations, and technical protection mechanisms associated with healthcare information systems, including electronic health records (EHRs), Internet of Medical Things (IoMT) devices, hospital networks, telemedicine platforms, and cloud-based healthcare infrastructures. To reflect both recent developments and established research trends, studies published between 2021 and 2025 were considered.

3.2. Literature Search Strategy

A structured literature search was conducted using major academic databases, including IEEE Xplore, Scopus, Web of Science, PubMed, and Google Scholar. These sources were

selected to provide broad coverage across engineering, computer science, and healthcare-oriented research. The search strategy used a combination of keywords and Boolean operators aligned with the study scope, such as "healthcare cybersecurity," "data privacy in healthcare," "medical IoT security," "insider threats," "ransomware in healthcare," "health information systems security," and "privacy-preserving techniques." Only English-language publications were considered to ensure consistency of interpretation and synthesis.

In addition to database searching, relevant records were also identified via other methods (e.g., selected websites and organizations) when they met the inclusion criteria.

3.3. Data Handling and Study Selection

The study selection process followed a PRISMA-ScR–aligned workflow consisting of identification, screening, eligibility assessment, and final inclusion. Records retrieved from all sources were merged and deduplicated prior to screening. Titles and abstracts were screened to remove publications clearly unrelated to healthcare cybersecurity or data privacy. Full-text reports were then assessed for eligibility using predefined inclusion and exclusion criteria. A PRISMA-style flow diagram is provided to summarize the selection process and enhance transparency.

3.4. Inclusion and Exclusion Criteria

To ensure relevance and consistency, predefined inclusion and exclusion criteria were applied during screening and full-text eligibility assessment.

3.4.1. Inclusion Criteria

- Peer-reviewed journal articles and conference papers.
- Studies focusing on cybersecurity threats and/or data privacy issues in healthcare systems.
- Publications proposing, analyzing, or reviewing technical, regulatory, or organizational security solutions in healthcare contexts.

3.4.2. Exclusion Criteria

- Non-peer-reviewed articles (e.g., editorials, opinion pieces, news items).
- Studies not specific to healthcare security or privacy.
- Duplicate publications or papers lacking sufficient technical or analytical detail to support synthesis.

3.5. Data Extraction and Synthesis

From each included study, key information was extracted, including the cybersecurity threat type, privacy issue addressed, healthcare application domain, proposed solution(s), evaluation setting (e.g., dataset/simulation/real deployment), and key findings. The evidence was charted and qualitatively synthesized into thematic categories, including threat classification, privacy challenges, regulatory considerations, and mitigation techniques.

3.6. Quality and Bias Considerations

Consistent with scoping review methodology and the heterogeneity of study designs in healthcare cybersecurity (e.g., surveys, simulations, synthetic datasets, prototypes, and deployment reports), this review did not exclude studies using a single formal risk-of-bias tool or quantitative quality score. Instead, to support transparent interpretation and reduce citation bias, we extracted and reported evidence characteristics and limitations where available (e.g., dataset realism: synthetic vs. real-world, evaluation metrics, reproducibility details, and stated assumptions). This approach supports evidence mapping while acknowledging variability in methodological rigor across the included literature.

3.7. PRISMA-ScR–Aligned Review Process

This review follows a PRISMA-ScR-aligned framework to enhance transparency and reproducibility in the literature selection process. Figure 2 summarizes the identification, screening, eligibility assessment, and final inclusion stages.

The database and register search identified 1285 records from databases and an additional five records from registers (total $n = 1290$). After removing duplicate records ($n = 510$), 780 records remained for title and abstract screening, during which 642 records were excluded for not meeting the predefined criteria. Full texts were sought for 138 reports; 23 reports could not be retrieved. The remaining 115 reports were assessed for eligibility through full-text review. At this stage, 63 reports were excluded for the following reasons: not focused on cybersecurity in healthcare ($n = 36$), conference poster/non-research format ($n = 21$), and insufficient data or missing outcome ($n = 6$). Ultimately, 52 studies met the inclusion criteria and were included in the review, as shown in Figure 2.

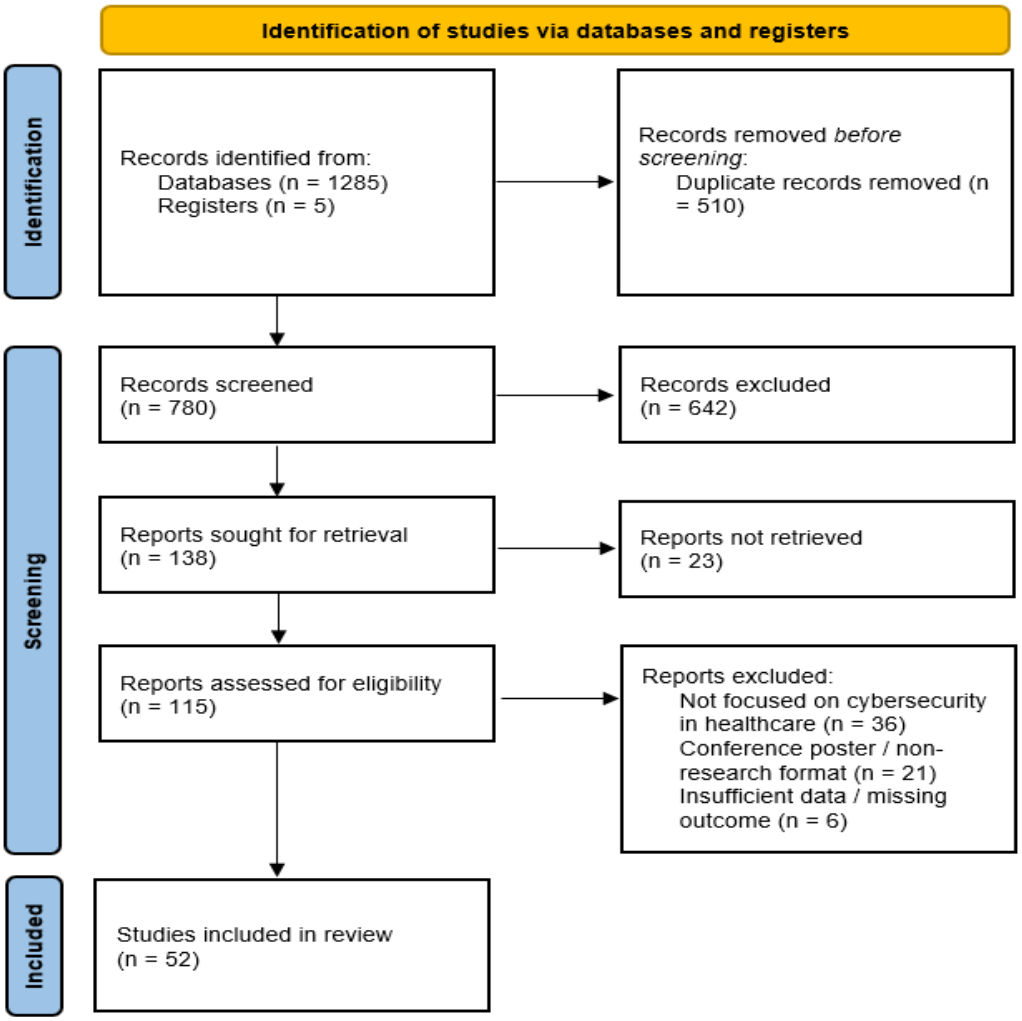

Figure 2. PRISMA flow diagram.

4. Cybersecurity Threat Landscape in Healthcare

Healthcare has become one of the most consistently targeted sectors for cyberattacks, driven by the high monetary and intelligence value of medical data and the critical requirement for uninterrupted service delivery. Cyber threats in healthcare encompass a wide range of attack vectors, including ransomware, malware, phishing, data exfiltration, and the exploitation of device-level vulnerabilities capable of compromising entire hospital networks [17]. These risks are further intensified by the sector's increasing re-

liance on distributed infrastructures, remote access systems, and continuously connected medical devices.

Certain data-driven sectors, including healthcare, finance, and critical infrastructure, are repeatedly targeted by cyber adversaries because of the sensitive and high-value information they manage. Among these, healthcare institutions are especially vulnerable to data breaches and ransomware incidents, which can disrupt clinical services and jeopardize patient confidentiality. Financial institutions face persistent threats aimed at stealing financial data or disrupting services, while critical infrastructure sectors, such as energy and transportation, are vulnerable to attacks that could cause widespread disruption. As cyber threats continue to evolve, enterprises in all industries must adapt their cybersecurity strategies to address emerging risks, from new attack vectors to increasingly sophisticated adversaries [18].

However, healthcare information systems are always exposed to serious security threats due to the highly sensitive and confidential data they contain [19], which can lead to violations of patient privacy, disruption of treatment, and even irreparable damage to the health and reputation of healthcare facilities. These threats include a variety of cyberattacks that specifically target vulnerabilities in these systems to gain access to data or disrupt system functionality.

In many cases, adversaries exploit weaknesses in hardware, operating systems, communication protocols, or security policies. Medical devices may contain default passwords, outdated firmware, or communication channels lacking encryption, enabling attackers to infiltrate systems through seemingly isolated endpoints. Once compromised, these devices can serve as lateral movement vectors to access additional assets within the healthcare network [20].

Threats in healthcare arise not only from external cybercriminals but also from unintended internal actions such as misconfigurations, weak authentication practices, and human error. Studies emphasize that healthcare operational workflows are particularly susceptible to insider mistakes because staff may prioritize usability and rapid system access over strict security procedures during demanding clinical operations [21].

Beyond operational disruption, cyber attacks can endanger patient safety. Compromised systems may lead to altered diagnostic data, malfunctioning medical devices [21], delayed treatment, or loss of access to patient histories, increasing clinical risks. Recent documented incidents have shown that service shutdowns due to cyber attacks can affect emergency services, daily operations, laboratory systems, and even surgical schedules, revealing the direct and tangible consequences of cyber security in healthcare.

Healthcare systems are exposed to two primary categories of security threats: insider threats and outsider threats. Insider threats originate from individuals with authorized access to healthcare systems, such as clinicians, administrative staff, or IT personnel, and may result from malicious intent, negligence, or compromised credentials, leading to unauthorized data disclosure or system misuse. In contrast, outsider threats are perpetrated by external adversaries who lack legitimate system access, including hackers, cyber criminals, and organized attack groups, and commonly manifest as malware infections, phishing campaigns, ransomware attacks, or denial-of-service incidents. Both insider and outsider threats pose serious risks to the confidentiality, integrity, and availability of sensitive healthcare data and services, underscoring the necessity for comprehensive and robust security mechanisms in healthcare environments.

4.1. Insider Threats

In addition to external adversaries, internal actors, including employees and contractors, may contribute to system compromise through negligence, policy violation, or ma-

licious intent. Human error continues to be a major factor in healthcare breaches, often caused by mis-configurations, insecure password practices, improper access control, or failure to follow cyber security protocols.

Insider threats in hospital networks are particularly challenging due to attackers' legitimate access privileges and the highly sensitive nature of healthcare data. Since their actions can look similar to normal clinical activity, harmful behavior, whether deliberate (such as data theft or sabotage) or accidental (such as careless handling of records, password sharing, or compromised accounts), may go unnoticed until damage has occurred. These incidents can undermine patient confidentiality, disrupt services, and expose organizations to regulatory penalties. Reducing insider risk typically requires a layered approach, combining least-privilege access and role-based controls with multi-factor authentication, detailed audit logging, and continuous monitoring to spot unusual patterns. Many hospitals also use anomaly detection methods to flag suspicious access behavior, alongside zero-trust practices that re-check trust throughout a session. Ongoing staff awareness training, clear procedures, and well-tested incident response plans are equally important for limiting both the likelihood and impact of insider-related breaches.

There are three main types of insider threats in healthcare systems, as illustrated in Figure 3, each characterized by distinct motivations and risk patterns. The types of insider attacks are outlined below.

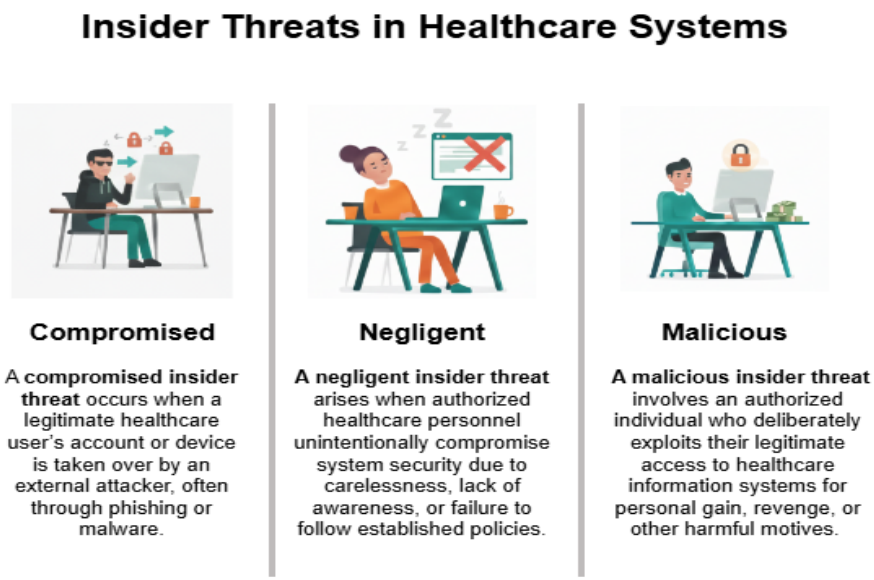

Figure 3. Insider threats in healthcare systems.

- Malicious Insiders: Malicious insiders are authorized users who intentionally misuse their access to harm healthcare systems or organizations. In healthcare environments, such threats often involve the deliberate theft of electronic health records (EHRs), intellectual property, or research data for financial gain, espionage, or personal motives. Studies report that malicious insiders may engage in data ex-filtration, system sabotage, or unauthorized disclosure of patient information, posing serious risks to patient privacy and institutional reputation. Although less frequent than other insider threat types, malicious insiders typically cause disproportionately high financial and reputational damage due to their deep system knowledge and privileged access. Detecting malicious insiders is challenging because their actions often resemble legitimate operational behavior until damage has occurred.
- Negligent Insiders: Negligent insiders are legitimate users who unintentionally cause security breaches due to carelessness or insufficient awareness. This category includes

incidents such as lost devices, misdirected information, or improper handling of sensitive data. A common example is an employee accidentally sending PHI to the wrong recipient or failing to encrypt data. Although these actions are unintentional, they can be frequent, particularly among overburdened staff [22]. In healthcare systems, negligent behavior includes weak password practices, accidental data disclosure, improper configuration of systems, and falling victim to phishing attacks. Literature consistently identifies negligent insiders as the most common cause of healthcare data breaches, largely due to the complex workflows, high workload, and stress experienced by healthcare staff. Such incidents frequently result in large-scale exposure of sensitive patient data and regulatory non-compliance. Unlike malicious insiders, negligent insiders do not intend harm, making training, awareness programs, and usability-focused security controls critical for mitigation.

- Compromised Insiders: Compromised insider threats occur when attackers hijack legitimate user credentials, often through phishing, malware, or credential theft. In healthcare environments, compromised accounts are particularly dangerous because attackers gain access to sensitive systems while appearing as trusted users. Research shows that compromised insiders are responsible for a significant portion of large-scale healthcare breaches, as attackers can move laterally across networks, access EHRs, and deploy ransomware. These threats blur the boundary between insider and outsider attacks, as external adversaries operate under internal identities. Effective mitigation requires multifactor authentication, continuous behavior monitoring, and anomaly detection, as traditional perimeter-based defenses are insufficient.

Existing Mitigation Approaches for Insider Threats

Insider threats remain one of the hardest security problems for healthcare organizations because harmful actions can originate from users who already have legitimate access to clinical systems. As a result, many hospitals rely on a combination of technical controls, monitoring practices, and organizational policies to reduce the likelihood of misuse and to limit damage when incidents occur. The following section reviews existing mitigation approaches that are commonly adopted to prevent, detect, and respond to insider-driven risks in healthcare environments.

Compared with baseline approaches, the proposed lightweight architecture [23] maintains strong insider-threat detection performance while substantially lowering computational overhead, making it suitable for resource-constrained hospital environments. It combines behavioral monitoring with GIS-based contextual cues and an efficient boosted ensemble to balance accuracy with practical feasibility. At the same time, the method still depends on labeled training data and may face difficulties when policies or user behavior change over time, particularly for dynamic policy enforcement. Future work should therefore focus on improving generalization through real-world clinical validation and exploring extensions such as federated learning for scalable training across institutions and explainable AI components to enhance transparency and trust.

Human-centered approaches emphasize education and organizational culture to reduce insider threats. Security awareness training is widely advocated in healthcare settings and typically addresses password hygiene, phishing recognition, secure data handling, and device protection. Tailoring training programs to specific roles enhances their effectiveness; for example, clinicians often benefit from scenario-based simulations aligned with real clinical workflows. Effective awareness initiatives promote vigilance without adding excessive burden to daily tasks. Complementary measures include managing staff stress and fatigue since overwork increases the likelihood of errors and providing clear, accessible channels for reporting phishing attempts or security concerns [22].

Newman et al. introduced an Advanced Privacy-Preserving Decentralized Federated Learning (APPDFL) framework [24] designed to address insider threat detection in collaborative healthcare settings. The framework adopts a serverless, peer-to-peer federated learning architecture enhanced with differential privacy, allowing multiple healthcare institutions to collaboratively learn threat patterns without sharing raw or sensitive data. The proposed method was evaluated using several versions of the CERT insider threat dataset (r4.2, r5.2, and r6.2) and was compared with conventional machine learning models, modern techniques, and centralized federated learning approaches under consistent experimental conditions. The results indicate that APPDFL delivers improved detection performance while ensuring privacy preservation and robust noise tolerance, demonstrating the practicality and effectiveness of privacy-aware cross-institutional collaboration in compliance with security and regulatory requirements.

The study addressed the increasing frequency of healthcare data breaches by examining both insider and outsider threats and the vulnerabilities within internal security systems [25]. Unlike prior work that mainly analyzed breach trends, it focused on the descriptive narratives reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Using text mining and visualization techniques, the study analyzed insider threats, system vulnerabilities, breach incidents, their impacts, and organizational responses across three types of data breaches, offering deeper insights into the underlying causes and consequences of healthcare data breaches.

Prior literature emphasizes that mitigating insider threats in healthcare requires a strong focus on human factors alongside technical controls. Key strategies include clear function allocation and task analysis to ensure that roles, responsibilities, and access privileges are well defined and aligned with job functions, reducing misuse and error [26]. Human error analysis is used to identify points where negligence, fatigue, or lack of awareness may lead to security incidents, enabling proactive redesign of workflows and policies. The use of modeling approaches such as UML use–misuse case diagrams, security sequence diagrams, and class diagrams supports early identification of accidental and malicious insider behaviors during system design. Continuous monitoring of user access, regular review of employee and third-party privileges, and integrating human-centered security considerations into system development are highlighted as essential measures for reducing insider-related data breaches in Healthcare 5.0 environments [27].

Healthcare data are increasingly stored in cloud-based infrastructures to support scalability and remote access, making robust security mechanisms essential to protect sensitive patient information from unauthorized access and insider threats. Ref. [28] investigated the growing risk of insider threats in cloud-based Database as a Service (DBaaS) environments, where complex data dependencies can be exploited by insiders to infer sensitive information. To address limitations of existing access control approaches, such as poor scalability, weak authentication, and insufficient insider tracking, the authors proposed a distributed access control framework that integrates blockchain-based authentication and insider activity monitoring [26]. Experimental results and a real-world case study demonstrated that the proposed framework is effective, scalable, and well-suited for dynamic cloud environments, even in the absence of standardized datasets.

4.2. Outsider Threats

Healthcare organizations increasingly face sophisticated external attacks, including phishing, ransomware, malware propagation, unauthorized network intrusion, and denial-of-service attacks. Such incidents are motivated by the high market value of medical information and the operational damage that can be inflicted by disabling clinical systems.

The threats listed below represent common types of outsider attacks in healthcare systems, as illustrated in Figure 4.

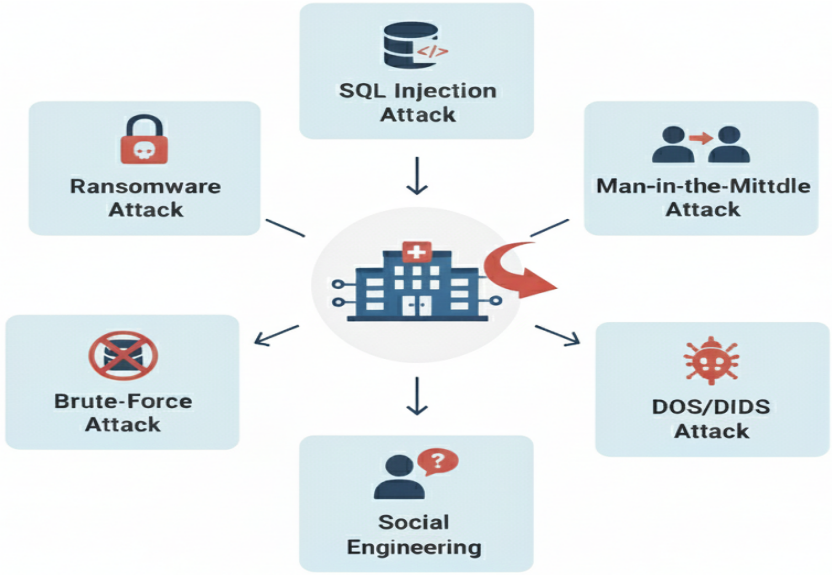

Figure 4. Outsider threats in healthcare systems.

- Malware: In healthcare environments, malware represents a class of cyber threats involving harmful software intended to disrupt system functionality, extract sensitive patient information, or obtain unauthorized access to clinical networks and medical devices. Typical malware variants include ransomware, spyware, and trojans, which can interfere with electronic health records (EHRs), impair critical healthcare services, and pose direct risks to patient safety [29]. The extensive use of interconnected devices, along with the presence of legacy systems, further increases the susceptibility of healthcare infrastructures to malware-based attacks, making them a significant cybersecurity concern.
  Malware attacks generally involve the creation and deployment of malicious code or firmware that infiltrates systems under the guise of legitimate software. Once introduced, such code can manipulate or destroy data, perform intrusive actions, or otherwise compromise the confidentiality, integrity, and availability of system resources. Common malware categories include viruses, worms, trojan horses, rootkits, and other forms of malicious code capable of penetrating healthcare information systems [30].
- Social Engineering/Phishing: Social engineering exploits the predictability of human behavior and plays a role in the majority of cyberattacks. It is also the fastest-growing attack vector, often described as increasing at an unprecedented rate. Social engineering is closely associated with data breaches, with approximately 95% of incidents linked to human error. The healthcare sector is particularly vulnerable, experiencing the highest average cost per breach, exceeding USD 7 million, surpassing all other industries. Globally, the projected economic impact of social engineering-related cyberattacks is expected to reach USD 10.5 trillion annually by 2025 [31].
- DoS/DDoS: The primary challenge facing m-health technologies is ensuring the security of medical and other sensitive data, with data availability being one of the most critical concerns. Distributed denial-of-service (DDoS) attacks pose a significant threat by disrupting continuous access to patient information and impeding data transmission across interconnected networks. Beyond data compromise, DDoS attacks

can severely restrict authorized users from accessing essential healthcare services and information portals [32].

Denial-of-service (DoS) attacks aim to disrupt services by overwhelming networks with excessive traffic, thereby preventing legitimate users from accessing critical systems. Such attacks can significantly degrade or completely shut down healthcare networks, severely impacting operational continuity. For instance, a DoS attack in 2014 temporarily disabled the administrative systems of Boston Children's Hospital, resulting in substantial operational and financial losses. Beyond economic damage, these attacks critically hinder healthcare providers' ability to access, transmit, and manage essential patient information during the attack period, posing serious risks to patient care and safety [31].

- Network Intrusion: Network intrusion in healthcare systems represents a critical cyber security threat due to the highly interconnected nature of modern clinical environments and the sensitivity of medical data. Attackers exploit vulnerabilities such as weak network configurations, un-patched systems, insecure remote access, and compromised credentials to gain unauthorized access to hospital networks [33]. Once inside, intrusions can enable lateral movement across clinical and administrative systems, allowing adversaries to ex-filtrate patient data, deploy ransomware, disrupt medical devices, or manipulate health records. These incidents not only compromise patient privacy but can also interrupt clinical workflows, delay diagnoses or treatments and pose direct risks to patient safety. The growing adoption of cloud services, tele-medicine platforms and Internet of Medical Things (IoMT) devices further expands the attack surface, making robust intrusion detection systems, network segmentation, continuous monitoring and timely incident response essential components of healthcare cyber-security strategies.
- Brute Force: Brute-force attacks attempt to gain unauthorized access by repeatedly guessing username and password combinations. In-hospital management information systems, such attacks can lead to serious data breaches and financial losses due to the sensitivity of stored information. To mitigate these risks, healthcare organizations should enforce strong password policies, implement robust authentication and multi-factor authentication, encrypt patient data, and deploy effective monitoring and response mechanisms. These measures help secure hospital systems while ensuring the safe delivery of healthcare services [34].
- Ransomware: Healthcare remains one of the most cyber attack-prone sectors due to its rapid digital transformation and increasing reliance on interconnected healthcare services. This shift has exposed significant security vulnerabilities that are increasingly exploited by cyber criminals, with ransomware emerging as one of the most severe and rapidly growing threats. Ransomware attacks have escalated in frequency and sophistication in recent years, causing substantial operational and financial disruptions to healthcare organizations. This study presents a comprehensive survey of ransomware attacks in healthcare and systematically categorizes existing mitigation and prevention strategies, including blockchain-based solutions, software-defined networking, machine learning techniques, and other security tools. It also highlights the key challenges faced by researchers in designing effective ransomware defenses for healthcare systems. Overall, the study offers valuable insights for researchers, healthcare institutions, and cyber security practitioners working to strengthen information security in healthcare environments.

Table 1 summarizes prominent ransomware families targeting healthcare systems, highlighting their primary initial compromise vectors. It also outlines the corresponding payload execution strategies used to propagate, escalate privileges, and disrupt clinical operations.

Table 1. Initial infection and execution techniques of major healthcare ransomware.

Ransomware Family	Initial Compromise Vector	Payload Execution Strategy
WannaCry	Exploitation of un-patched SMB services (EternalBlue vulnerability)	Executes the ransomware payload by encrypting local files using embedded cryptographic routines after successful exploitation, followed by optional self-propagation via SMB scanning.
Locky	Phishing emails containing malicious document attachments	Embedded macros or scripts download and execute the ransomware binary on compromised hosts.
SamSam	Unauthorized access via weak RDP credentials or vulnerable web services	Performs privilege escalation and manually encrypts systems across the network using customized tools.
Ryuk	Phishing-based malware delivery through infected email attachments	Uses PowerShell or script-based loaders to deploy ransomware and enable lateral movement.
Maze	Social engineering via phishing emails carrying malicious files	Downloads the payload, encrypts local and shared files, and threatens public disclosure of stolen data.
Petya/NotPetya	Combination of SMB exploitation and phishing campaigns	Harvests credentials, leverages native tools (e.g., PsExec), and disrupts system boot processes.
Cerber	Email-based phishing attacks and exploit kits	Deploys ransomware via scripts or macros and communicates with distributed command-and-control servers.

- Man-In-The-Middle Attack: The healthcare sector is particularly vulnerable to man-in-the-middle (MitM) attacks due to the rapid adoption of Internet of Things (IoT) technologies in clinical environments. IoT-enabled healthcare applications, including electronic health records, telemedicine, telesurgery, mobile health, and remote patient monitoring, have significantly improved service delivery but have also expanded the attack surface. Modern hospitals deploy thousands of network-connected devices, averaging approximately 17 devices per hospital bed. Despite this growth, many medical IoT devices lack robust security mechanisms such as strong encryption and secure authentication [35].

  According to an industry analysis reported by Ordr [36], approximately 15–19% of IoMT devices deployed in healthcare environments continue to operate on Windows 7, an operating system that has reached end-of-life and no longer receives security updates. This estimate is derived from telemetry data collected across healthcare deployments primarily in North America and Europe, rather than a fully global sample. The continued use of unsupported operating systems significantly increases the attack surface of IoMT infrastructures, exposing medical devices to known vulnerabilities and facilitating cyberattacks such as ransomware, data breaches, and man-in-the-middle (MitM) attacks. These risks are further exacerbated by resource-constrained medical sensors and insecure wireless communication protocols, making robust security mechanisms essential for ensuring data confidentiality, integrity, and availability in IoMT systems.

  In an IoMT environment, a man-in-the-middle (MitM) attack arises when an adversary successfully positions itself between medical sensors and a local processing unit (LPU), such as a smartphone, tablet, or gateway. This positioning is typically achieved by exploiting weaknesses in short-range wireless communication protocols, including Bluetooth Low Energy, in combination with the limited computational resources and security mechanisms available on medical sensors. As a result, the attacker gains unauthorized access to the communication channel without being detected by either endpoint [37]. After establishing this intermediary position, the attacker can passively monitor the exchanged physiological data, including parameters such as heart rate,

blood pressure, and oxygen saturation, thereby compromising patient confidentiality. More critically, the attacker may actively manipulate communication by modifying or replaying transmitted data. In emergency scenarios, abnormal physiological measurements can be replaced with previously recorded normal values before reaching the LPU, causing the monitoring system to incorrectly interpret the patient's condition and suppress the generation of medical alerts.

The threat is further amplified by the availability of off-the-shelf tools that enable the interception and manipulation of wireless traffic over distances exceeding the typical operating range of IoMT devices. Even when encryption is employed, flaws in device pairing, key establishment, and authentication procedures may allow attackers to decrypt messages or inject forged packets. Consequently, MitM attacks represent a severe risk in IoMT systems, as they compromise not only data privacy but also data integrity and the reliability of real-time clinical decision-making.

- SQL Injection: SQL injection is a significant cyber security threat to healthcare systems due to the extensive use of web-based applications such as electronic health records, patient portals, and billing platforms that rely on backend databases [38]. This attack occurs when malicious SQL code is inserted into input fields and executed by poorly secured applications, allowing attackers to access, modify, or delete sensitive data. In healthcare environments, successful SQL injection attacks can lead to unauthorized disclosure of protected health information, corruption of medical records, disruption of clinical services, and violations of regulatory requirements such as HIPAA [39]. The presence of legacy systems, inadequate input validation, and insufficient access controls further increases the susceptibility of healthcare organizations to such attacks. Consequently, mitigating SQL injection risks through secure coding practices, including parameterized queries, rigorous input validation, and regular security assessments, is essential to ensuring data integrity, patient safety, and trust in digital healthcare infrastructures.

Table 2 compares existing cybersecurity and privacy-preserving solutions in healthcare based on their problem focus, proposed techniques, and addressed attack types. It also highlights evaluation methods and key performance outcomes reported in prior studies.

Table 2. Summary of cybersecurity and privacy protection approaches in healthcare systems.

Ref	Problem Focus	Proposed Approach	Attacks / Threats	Data / Evaluation Highlights
[40]	Protecting smart-health and personal medical device (PMD) data integrity	Blockchain-enabled framework integrating IPFS, FHIR APIs, and a GAN-based intrusion detection system for monitoring PMD communication	DoS, replay attacks, man-in-the-middle (MitM), false data injection	Approximately 98.7% detection accuracy with an F1-score close to 98% across multiple attack scenarios
[41]	Cyberattack detection in healthcare cyber-physical systems (HCPSs)	Cognitive machine learning assisted attack detection framework (CML-ADF) supporting secure data sharing and intelligent threat prediction	DoS, sniffing, routing attacks, impersonation, code injection	Achieves 98.2% accuracy and a 96.5% attack prediction rate with reduced communication overhead

Table 2. *Cont.*

Ref	Problem Focus	Proposed Approach	Attacks / Threats	Data / Evaluation Highlights
[42]	Availability protection for mobile healthcare (m-health) cloud systems	Novel DDoS detection and prevention algorithm evaluated in a cloud-based simulation environment	Distributed denial-of-service (DDoS) attacks	Simulation results demonstrate effective DDoS detection and mitigation
[43]	Privacy preservation of patient data in smart hospitals	Cyberattack prevention framework employing two-factor authentication (OTP and CAPTCHA), encrypted credentials, and role-based access control	Unauthorized access, credential compromise, spamming	Design-oriented evaluation emphasizing enhanced privacy and access control mechanisms
[44]	Secure storage and transmission of healthcare data during large-scale digitization	Cryptography-based data protection approach using AES, DES, 3DES, and RSA algorithms	General cyber threats against digital healthcare data	Conceptual analysis and comparison of cryptographic techniques without experimental benchmarking
[32]	Prediction and mitigation of healthcare data breach risks	Gradient boosting—a predictive model for assessing the severity of healthcare data breaches	Hacking incidents, network/server breaches, IT-related attacks	Evaluated using datasets from the US Department of Health and Human Services and Kaggle, demonstrating strong predictive performance

Existing Mitigation Approaches for Outsider Threats

The rapid adoption of the Internet of Medical Things (IoMT) has increased cybersecurity risks, as many medical devices and their supporting software are not designed to withstand internet-based attacks. To address this challenge, the authors propose a cyberattack and anomaly detection framework [45] that integrates recursive feature elimination (RFE) with a multilayer perceptron (MLP) classifier. Optimal features are selected using logistic regression and extreme gradient boosting–based kernels, while model performance is enhanced through hyperparameter optimization and 10-fold cross-validation. The proposed approach is evaluated on multiple IoMT and healthcare cybersecurity datasets and achieves high detection accuracy across diverse environments. These results demonstrate the effectiveness of machine-learning-based anomaly detection for improving the security and resilience of IoMT-enabled healthcare systems.

Cybersecurity is a critical concern for healthcare organizations, which are among the most vulnerable to cyberattacks. Protecting medical records is essential due to their sensitive personal and financial content. This study [46] analyzed 352 real-world cyberattacks on healthcare institutions using Common Vulnerability Scoring System (CVSS) data and applied machine learning techniques to model vulnerabilities in healthcare IT and industrial control systems. Results showed consistently high vulnerability scores, particularly in institutions with prior attacks and no mitigation measures. Among the evaluated models, the K-nearest neighbors (KNN) algorithm achieved the best performance and was further used to predict future cyberattacks. The findings highlight the high risk facing healthcare systems and emphasize the urgent need for stronger cybersecurity measures.

The integration of technologies of the Internet of Things (IoT) into e-Health systems has significantly improved healthcare services but has also introduced serious security challenges [47]. In particular, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks pose a critical threat to the availability and reliability of IoT-based e-Health servers, potentially disrupting real-time patient monitoring. This work reviews existing

DoS/DDoS mitigation approaches in IoT environments and proposes a reliable solution to improve the resilience of e-Health servers against such attacks.

The authors proposed [34] a cybersecurity framework for hospital management information systems (HMISs) aimed at mitigating brute force and related cyberattacks. The model integrates layered security mechanisms, including strong authentication, access control, encryption, firewalls, and intrusion detection systems, to protect sensitive patient data. To specifically counter brute force attacks, the framework employs multifactor authentication, account lockout policies, CAPTCHA verification, API key enforcement, and continuous system monitoring. The architecture emphasizes least-privilege access, regular patching, and real-time threat detection. Experimental evaluations demonstrated that the proposed HMIS model outperforms existing approaches in terms of threat detection accuracy, security management, and information management, highlighting its effectiveness in improving resilience against cyberattacks in healthcare environments.

The paper proposed several practical countermeasures to mitigate SQL injection threats in medical systems, emphasizing the importance of a layered defense strategy. Infrastructure separation, such as isolating SQL database servers from Internet-facing web servers through the use of a demilitarized zone (DMZ) and an effective firewall, is recommended to reduce direct exposure to external attacks [48]. Input or data sanitization is identified as a critical preventive measure, where malicious SQL characters are filtered or safely substituted before query execution to prevent syntactic manipulation of database commands [49]. The paper also highlights the importance of strict SQL database permissions, advocating least-privilege access control through role-based permissions and database views to limit the potential damage of successful injection attempts [50]. Furthermore, reducing customization and reliance on dynamic SQL queries by using stored and pre-tested procedures is suggested to minimize opportunities for malicious query injection while improving performance [51]. Finally, system audit and monitoring are recommended to detect abnormal database behavior, such as unusual query loads or access patterns, enabling the early identification of potential SQL injection attacks [52].

4.3. Blockchain Based Security Solutions

This qualitative study examined how healthcare organizations build digital resilience as they digitalize. It identified four interdependent constructs knowledge and resources, resilience approaches to uncertainty, inter-dependencies, and cyber security resilience, and argued that digital transformation requires senior-management commitment to balance resource investment with cyber security risk. Managers are encouraged to adjust their strategies as knowledge resources and threats evolve. The study provided a clear conceptual framework linking digital transformation and resilience, offering boards guidance on aligning investment and security measures [53].

Ref. [40] proposed a combination of a generative adversarial network (GAN) and blockchain to detect DDoS and spoofing attacks on smart PMDs. The GAN trained a discriminator to identify abnormal traffic, and the blockchain immutably logged device identities and alerts. Simulation results showed detection accuracy above 98% across multiple attack types. High accuracy and low false-positive rates demonstrated the efficacy of using GANs with blockchain to secure PMDs. However, experiments were limited to simulated PMD traffic; real-world deployment may face delays from blockchain transaction times and require more heterogeneous datasets.

The authors designed a layered smart-healthcare architecture combining blockchain with AI-based malware analysis [54]. IoT devices sent encrypted data to fog nodes; a machine-learning module using random forest and logistic regression classifiers achieved 93.14% malware detection accuracy. The blockchain stored hash values of verified transac-

tions to ensure integrity and auditability. An open issues section highlighted that advanced attacks such as Rowhammer, buffer overflow, and phishing remained challenging and that the energy consumption and scalability of blockchain networks needed to be improved. Integrating AI detection with blockchain provided an auditable and moderately accurate (≈93%) defense against malware in smart healthcare. The architecture is not yet resilient to sophisticated hardware and social-engineering attacks and still suffers from the high energy consumption and scalability limitations of conventional blockchain networks.

Ref. [55] introduced a federated-learning scheme that uses secure multi-party computation (SMPC) and blockchain to verify local models and defend against poisoning. Hospitals trained local models on private data; a blockchain ledger verified the encrypted model updates and rejected poisoned contributions. Experiments showed that the secure verification preserved inference time and could recover up to 25% of lost global accuracy when models were poisoned. The authors planned to design more efficient consensus mechanisms and support heterogeneous local models.

The authors proposed a secure IoT framework for smart healthcare that applies min-max scaling [56], the ReliefF algorithm for feature selection, an autoencoder for intrusion detection, and a temporal convolutional network (TCN) for classification. Blockchain was used to record transactions and enhance trust among devices. The combination of an autoencoder and TCN aimed to improve detection accuracy and efficiency. Integrating advanced feature selection with autoencoder-TCN models enhanced both accuracy and computational efficiency in a blockchain-secured environment. The paper focused on simulated data; the computational complexity of combining autoencoders and TCNs with blockchain was not discussed, and a real-world evaluation was needed.

Ref. [57] proposed a hybrid intrusion-detection model for IoT healthcare networks. Features were selected using the Ant-Lion Optimizer, a hybrid convolutional neural network–LSTM (CNN-LSTM) detected anomalies, and a blockchain recorded events. Simulation results showed high detection accuracy, precision, F1-score, and recall, outperforming baseline models. The authors noted that future work should test the approach on real hardware and improve efficiency. The hybrid CNN-LSTM with Ant-Lion-based feature selection and blockchain integration achieved superior intrusion-detection performance and low false positives. However, evaluations were purely simulated; real-world deployment could reveal latency and resource-consumption issues, and optimization was needed for deployment on resource-constrained medical devices.

The proposed approach in [58] introduced a permissioned blockchain with a reputation-based mining (RBM) algorithm and a stacked non-negative autoencoder (SNNA) to verify data reliability and detect malicious nodes in industrial healthcare systems. Experiments indicated that PBDL achieves higher classification accuracy and lower false positives than traditional methods while reducing computation and communication overhead thanks to the permissioned blockchain. Combining a lightweight permissioned blockchain with deep-learning-based reliability classification yielded efficient and accurate detection of malicious nodes.

The authors of the framework in Ref. [59] used the Gini index to rank the trustworthiness of nodes and integrated blockchain to detect and punish grayhole/blackhole attacks in healthcare cyber-physical systems. Simulation results showed that compared with a baseline BCPS-RPL method, GBG-RPL reduced the packet-loss ratio by 7.18%, increased residual energy by 11.97%, reduced message overhead by 21.65%, and decreased end-to-end delay by 28.34%.

4.4. ML/DL Based Security Solutions

In [60], the authors proposed a quantum machine-learning scheme for classifying user behavior in IoT networks. A fuzzy Gaussian quantile neural network was combined with a deep variational adversarial encoder to learn features from user traffic. The model was evaluated on two cybersecurity datasets: UNSW NB15 and Bot-IoT. On UNSW NB15, it achieved about 95% overall accuracy and an F1-score of ≈70%, while on Bot-IoT, the accuracy increased to 98% with an F1-score of ≈75%. Because the paper has been retracted (issues with authorship and references), its results should be interpreted cautiously. Ref. [61] developed a blockchain-enabled IoT framework in which a convolutional neural network (CNN) authenticated users based on biometrics, while the AES cipher protected stored healthcare data. Using a small real-time dataset (100 subjects), the CNN achieved ≈95% precision/recall/F1 and ≈98% overall accuracy. The framework was designed for smart hospitals, but was tested only in a controlled environment.

The authors built a two-level privacy intrusion-detection system combining homomorphic encryption (Paillier), elliptic-curve Diffie–Hellman–Montgomery key exchange, and a permissioned blockchain. A neural network was trained on actual and encrypted versions of two datasets: ToN-IoT and IoT-Botnet. With the transformed (encrypted) ToN dataset, the model attained ≈90.86% accuracy; when trained on the actual dataset, it achieved ≈94.34% accuracy and a loss of 8.89. For the transformed IoT dataset, the two-level privacy model reached 99.58% accuracy with low loss (≈0.0167%), while the actual dataset yielded 99.89% accuracy. Class-wise precision, detection rate, and F1-score exceeded 90%, and the false-acceptance ratio was near zero. The scheme demonstrated high detection accuracy even when data are encrypted but relied on computationally heavy cryptographic operations [62].

Ref. [63] introduced a permissioned blockchain framework for securing IoT-based healthcare systems. It combines a hybrid deep-learning intrusion detector (CNN-LSTM) with homomorphic encryption, enabling encrypted traffic to be analyzed without decryption. A trust-evaluated network aggregator uses consensus updates and a dynamic trust rating before committing verified data to the blockchain. The paper focuses on architectural design and privacy preservation; while the authors discuss proof-of-concept experiments that reportedly improved throughput and latency, they do not provide explicit detection-accuracy or F1-score values.

Ref. [64] proposed GBG-RPL, a blockchain-assisted routing security framework designed to mitigate grayhole and blackhole attacks in healthcare cyber-physical systems. The approach integrated a Gini-index-based trust evaluation mechanism with a blockchain-enabled routing protocol to assess node behavior and enforce accountability in IoT-based healthcare networks. Trust scores derived from packet-forwarding behavior were recorded on the blockchain, enabling transparent identification and isolation of malicious nodes without relying on centralized authorities. The framework was evaluated through simulation, demonstrating improvements in key network performance metrics, including reduced packet loss, lower end-to-end delay, decreased control overhead, and improved residual energy compared with conventional RPL-based solutions. The results indicated that combining lightweight trust metrics with blockchain can enhance routing reliability and security in resource-constrained healthcare IoT environments while preserving network efficiency.

4.5. AI-Based Security Solutions

The proposed study presents an AI-driven architecture for securing IoT healthcare systems. It integrates elliptic-curve cryptography and an authentication protocol for device enrollment, then uses a CNN-based intrusion-detection engine with an adaptive LSTM

classifier. The blockchain layer stores encrypted event logs and trust scores, while a fuzzy-logic module provides dynamic trust management. Experiments on an intrusion-detection dataset show that the system detects normal traffic and DoS attacks with about 95% accuracy (e.g., 47,500 of 50,000 normal instances correctly detected and 28,500 of 30,000 DoS instances). Results show F1-scores of 0.95 for all major intrusion classes (DoS, Probe, R2L, and U2R). These results suggest high accuracy, but they are based on simulated datasets and may not reflect real-world heterogeneity [65].

Ref. [66] proposed a hybrid artificial intelligence framework for insider threat detection in hospital information systems (HISs) by integrating rule-based reasoning, machine-learning classifiers, and deep-learning-based anomaly detection. The framework analyzed heterogeneous hospital log data, including EHR access records, user activity traces, and network logs, and extracted behavioral, contextual, and temporal features reflecting normal and abnormal user actions. A rule engine captured explicit policy violations, while supervised models such as random forest or SVM identified known misuse patterns, and an LSTM/GRU-based autoencoder detected subtle temporal deviations in user behavior. These components were combined using a decision-fusion mechanism to generate final threat scores. Experimental evaluation using simulated hospital logs showed that the hybrid design reduced false positives and improved detection robustness compared with standalone rule-based or machine-learning approaches, highlighting the effectiveness of combining domain knowledge with data-driven behavioral modeling for insider threat mitigation in healthcare environments.

The proposed framework examined AI-driven cybersecurity mechanisms for protecting patient data and medical devices in modern healthcare systems, with a particular focus on threats arising from interconnected AI applications and Internet of Medical Things (IoMT) devices. The study discussed adversarial attacks on AI models, unauthorized access to electronic health records, ransomware incidents, and vulnerabilities in connected medical devices, and analyzed how AI itself can be leveraged for cybersecurity defense. Techniques such as AI-based anomaly detection, predictive analytics, encryption, authentication mechanisms, and blockchain-assisted data management were reviewed within a system-level architecture. The paper presented comparative analyses of different cyber-threat categories and reported effectiveness ranges for AI-based threat detection, anomaly detection, and predictive analytics based on incident statistics and simulated evaluations. Overall, the work emphasized the role of AI as both an attack surface and a defensive tool, underscoring the need for integrated technical, regulatory, and organizational measures to enhance cybersecurity resilience in AI-enabled healthcare systems [67].

4.6. Cryptography Based Security Solutions

In this study, the authors designed an IoT architecture where each sensor has a unique identity stored on a blockchain [68]. A trusted authority issued keys, and an identity-based signature (IBS) scheme authenticated data, while the hashed data were stored on a blockchain ledger to ensure confidentiality, integrity, and availability. Security features included scalability, confidentiality, integrity, access control, data privacy, and forward/backward secrecy. Swarm storage and AES encryption were used to improve performance. The architecture combined identity-based cryptography with blockchain to provide a scalable, privacy-preserving IoT healthcare system and resisted replay and man-in-the-middle attacks. It relied on a trusted authority to issue keys and store identities; blockchain and Swarm storage introduced extra latency and overhead.

Ref. [69] focused on secure and privacy-preserving sharing of health data across national borders. It introduced the SECANT framework, which combines proxy re-encryption, zero-knowledge proofs, and identity-based encryption to protect patient data and support

granular access control. The framework incorporated a privacy manager that anonymized data before storage and used a hybrid encryption scheme to allow authorized parties to re-encrypt data without decrypting it. A modular architecture and performance evaluation showed that proxy re-encryption can be integrated into eHealth systems while respecting regulatory requirements.

The authors proposed a quantum-enabled security architecture in which a quantum feed-forward neural network (QFNN) was embedded within a quantum-protected healthcare data communication unit. Quantum encryption was used to generate unconditionally secure keys, and the QFNN detected malicious requests before data transmission began. Experiments on four breach datasets show that incorporating quantum encryption and QFNN can increase detection accuracy compared with classical systems [70].

Mittal et al. designed an IoT architecture in which each medical sensor and doctor had a unique identity. Data were encrypted using identity-based encryption and decrypted by the intended recipient through a role-based proxy decryption (RBPD) method. The authors compared encryption/decryption time and energy consumption with conventional RSA/AES and reported that the proposed scheme reduced decryption time and power usage because only authorized attributes were decrypted. The architecture ensures forward secrecy and fine-grained access control without the need for repeated key distribution [71].

Rasheed and Kumar presented three lightweight encryption schemes tailored to resource-constrained IoT healthcare devices. The first uses a hybrid Q-matrix Fibonacci sequence combined with a one-dimensional hyper-chaotic system to improve confusion and diffusion; the second combines a 1D logistic–sine chaotic map; and the third applies a combined transformation and expansion (CTE) scheme. The schemes were evaluated using metrics such as unified average changed intensity (UACI), number of pixel change rate (NPCR), and cross-entropy, showing near-ideal values and low computational overhead [72].

Shinde et al. [73] proposed a cross-layer security framework that encrypts data at the MAC, network, and application layers and uses elliptic-curve cryptography for authentication. A trust-based routing mechanism mitigates blackhole and replay attacks. Simulations in NS-3 demonstrated improvements in packet delivery ratio, throughput, and energy efficiency compared with baseline routing. The study suggested that combining cryptographic techniques across layers can enhance security in smart-healthcare networks.

Table 3 presents a comparative analysis of existing cybersecurity approaches for healthcare systems, summarizing each study's method and technique, target problem and network model, dataset, evaluation metrics, and the key advantages and limitations reported.

The effectiveness of cybersecurity countermeasures in healthcare varies significantly depending on the threat model, system architecture, and deployment environment. Cryptographic techniques are highly effective in ensuring data confidentiality and integrity, but offer limited protection against insider threats and advanced persistent attacks. Machine learning-based intrusion detection systems demonstrate strong performance in identifying anomalous behavior and malware; however, their effectiveness can degrade due to data imbalance, concept drift, and limited availability of labeled datasets. Blockchain-based solutions enhance data integrity, traceability, and auditability, yet their scalability and latency remain challenging in large-scale healthcare deployments. Zero-trust architectures provide comprehensive protection by enforcing continuous verification and least-privilege access, particularly against insider threats, although their effectiveness depends on correct policy configuration and system integration. Hybrid approaches that combine multiple techniques generally offer higher overall effectiveness but introduce additional complexity and operational overhead.

Table 3. Comparison of existing cyber security approaches in healthcare systems.

Ref & Year	Methods	Techniques	Problem Focus	Network Model	Dataset	Evaluation Metrics	Advantages	Limitations
[53] (2023)	Blockchain-based IDS	GAN, blockchain	PMD attack detection	Smart PMD IoT network	Simulated PMD traffic	Accuracy >98%	High detection accuracy	Evaluated only on simulated data
[55] (2023)	Blockchain-secured IDS	CNN	Intrusion detection	IoT healthcare network	OCTMNIST, TissueMNIST	Accuracy, precision	Data privacy	High computational costs and energy resources
[68] (2021)	Blockchain-based authentication	IBS, AES, blockchain	Secure IoT authentication	IoT healthcare sensors	Hospital records	Qualitative analysis (scalability, integrity, and access control)	Strong access control	Relies on trusted authority
[57] (2022)	Blockchain-based IDS	ALO, CNN-LSTM	Intrusion detection	IoT healthcare	Simulated IoT data	Accuracy, F1-score	High IDS performance	Lacks real deployment
[58] (2022)	Permissioned blockchain	SNNA, RBM	Secure data sharing	Industrial healthcare	Proprietary data	Accuracy, FPR	Efficient data validation	Scalability not tested
[59] (2023)	Blockchain-based routing security	Gini index, blockchain	Grayhole attacks	Healthcare CPS routing	Simulated routing	PLR, delay, energy	Improved routing metrics	Blockchain overhead
[67] (2024)	Deep-learning IDS	CNN/LSTM, ECC	Intrusion detection and authentication	IoT medical sensors	NSL-KDD	Accuracy $\approx 95\,\%$, $F_1 \approx 0.95$	High accuracy	Benchmark-limited
[70] (2025)	Quantum security	Quantum encryption	Secure data management	Distributed hospitals	Hospital records	Accuracy up to 3.13–16.13% (maximum 67.6% improvement)	Improved confidentiality	High complexity; no blockchain
[72] (2025)	Lightweight chaotic-map encryption	Chaos theory, logistic map	Medical image security	Stand-alone system	Medical images	NPCR $\approx 99.6151\,\%$, UACI $\approx 38.8925\,\%$	Strong diffusion	Encryption-only; no IDS
[66] (2024)	Hybrid AI	ML/DL, encryption	Cyber-threat detection	IoT healthcare	Simulated log	not specified	Adaptive detection	Simulated data
[40] (2024)	Deep learning and blockchain-based	GAN, ANN, SVM, and KNN	Integrity attack detection	Smart health system	PMD communication traffic dataset	Accuracy >98%, $F_1 \approx 98\%$	High detection accuracy	Limited to four attacks

4.7. Research Gaps in Existing Literature

The reviewed literature proposes a variety of blockchain-enabled, cryptographic, and machine-learning methods for protecting healthcare IoT systems, yet several clear research gaps remain:

- Lack of real-world validation and cross-domain generalization: Most intrusion-detection or anomaly-detection frameworks are evaluated on synthetic or proprietary datasets. For example, a recent AI-driven IDS achieved high accuracy on NSL-KDD, but further tuning was needed to detect more complex attacks and operate with low latency. Others acknowledge that pilot deployments are required to test scalability and compliance in clinical settings. Real-world experiments, cross-institutional datasets, and longitudinal studies would strengthen evidence.
- Scalability and energy efficiency of blockchain-based solutions: Papers report strong security but also high computational overhead and transaction latency. Future work calls

for optimizing consensus mechanisms and partitioning techniques to handle growing healthcare data volumes. Lightweight blockchains or off-chain strategies are needed to support resource-constrained medical devices without compromising security.

- Handling heterogeneous and complex threat landscapes: Many IDSs focus on DoS/grayhole attacks and assume homogeneous sensor networks. One study explicitly highlighted that improving detection rates for more complex intrusions and reducing latency should be targeted. Broader threat models (e.g., multi-vector attacks, insider threats, side-channel exploits) and datasets reflecting diverse IoT devices are required.
- Privacy-preserving analytics and decentralized identity management: Several approaches rely on centralized key authorities or share raw data among participants. The survey on blockchain-AI integration identified privacy-preserving techniques (differential privacy, secure multi-party computation) as an area for future research. Developing self-sovereign identity frameworks and integrating zero-knowledge proofs could minimize trust assumptions.
- Integration of quantum technologies: Quantum-based cryptography frameworks are proposed but remain largely conceptual and lack practical evaluation. Research should explore how quantum key distribution or quantum-secure algorithms can interoperate with existing healthcare blockchains and IoT devices.
- Explainability and regulatory compliance: High-accuracy deep-learning models often behave as black boxes. There is little discussion on explainable AI to support clinical decision-making or on how systems meet regulations such as HIPAA or GDPR. One review emphasizes the need for regulatory compliance to be addressed before widespread adoption of localhost. Future work should incorporate interpretable models and formal compliance checking.
- Dynamic trust management and user-centric design: Although some frameworks incorporate trust scores or fuzzy logic, they do not account for changing contexts, biases, or the needs of clinicians and patients. More research is needed on adaptive trust management, human-factor evaluations, and usability studies to ensure secure systems are acceptable in practice.

In summary, while existing work demonstrates promising detection accuracy and secure architectures, significant research is still needed on real-world deployment, scalability, heterogeneous attack coverage, privacy preservation, quantum integration, explainable AI, and regulatory compliance.

Figure 5 illustrates the distribution of reported data breach threats in the U.S. healthcare sector from the year 2023. Ransomware constituted the largest share, accounting for 46% of reported incidents, highlighting its dominance as a primary cyber threat. Phishing attacks followed at 25%, reflecting the continued exploitation of human vulnerabilities. Insider threats represented 7% of cases, while application misconfigurations and unsecured databases each contributed 5%, indicating persistent weaknesses in system configuration and data management practices. The remaining 11% fell under other attack categories, underscoring the diverse and evolving nature of cyber risks faced by healthcare organizations [74].

Long-term healthcare data breach statistics reported by the HIPAA Journal reveal a sustained and accelerating increase in the scale of cybersecurity incidents affecting the U.S. healthcare sector over the past decade and a half. As shown in Figure 6, the number of exposed healthcare records remained relatively low between 2009 and 2014, reflecting fewer large-scale digital breaches during the early adoption of electronic health systems. However, from 2015 onward, the volume of compromised records rose steadily, followed by a sharp escalation after 2020, coinciding with increased digitization, cloud adoption,

and the proliferation of ransomware attacks. The trend peaked in 2024, with approximately 276 million records exposed, before declining in 2025 to around 57 million records. Despite this reduction, the overall trajectory demonstrates a persistent and growing threat landscape, characterized by periodic large-scale breach events [75].

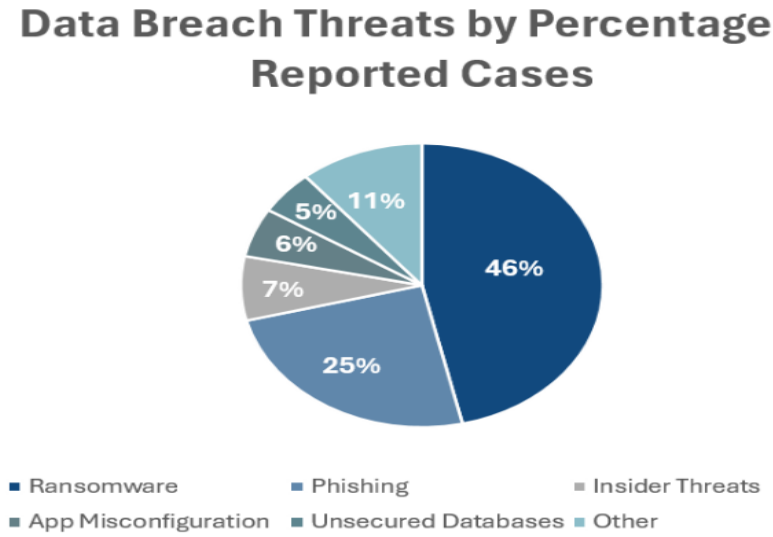

Figure 5. Distribution of data breach threats in the U.S. healthcare system by percentage of reported cases.

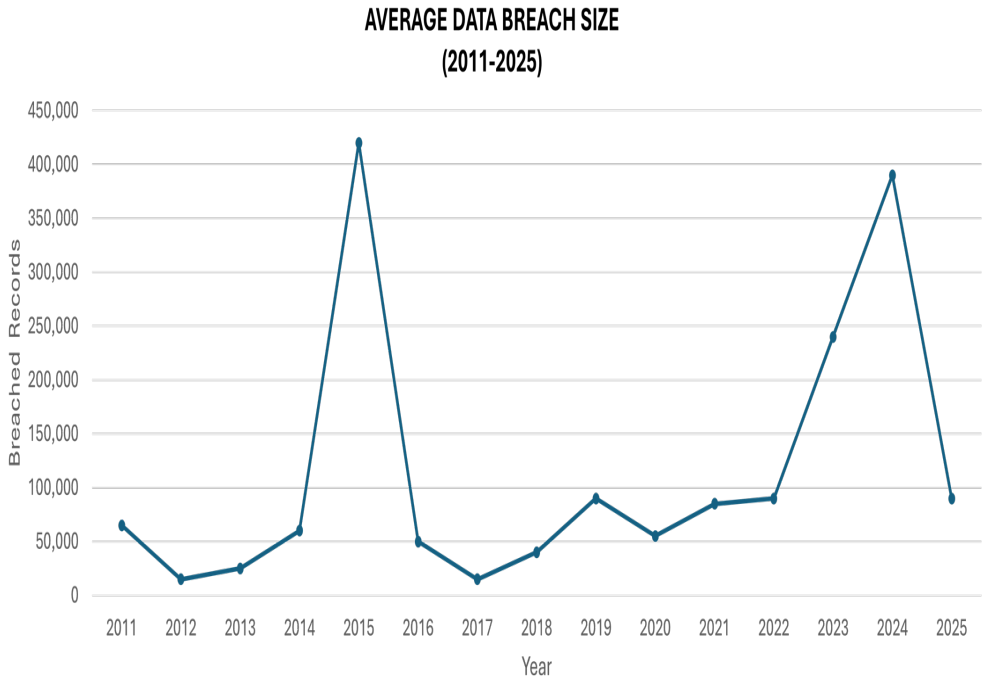

Figure 6. Trend of reported healthcare data breaches in the United States based on the number of breached records over the period 2011–2025.

Beyond the increasing scale of breaches, their economic impact on healthcare organizations remains exceptionally high [75]. As illustrated in Figure 7, the average cost of a healthcare data breach in 2025 reached approximately USD 7.42 million, substantially exceeding the global all-industry average of USD 4.44 million. This persistent cost disparity reflects the sensitivity of healthcare data, extended breach detection and containment timelines, regulatory penalties, and the operational disruption caused by cyber incidents. Although the average cost has shown a modest decline compared to previous years, health-

care continues to be the most financially impacted sector, underscoring the critical need for proactive cyber security measures and robust data privacy protections.

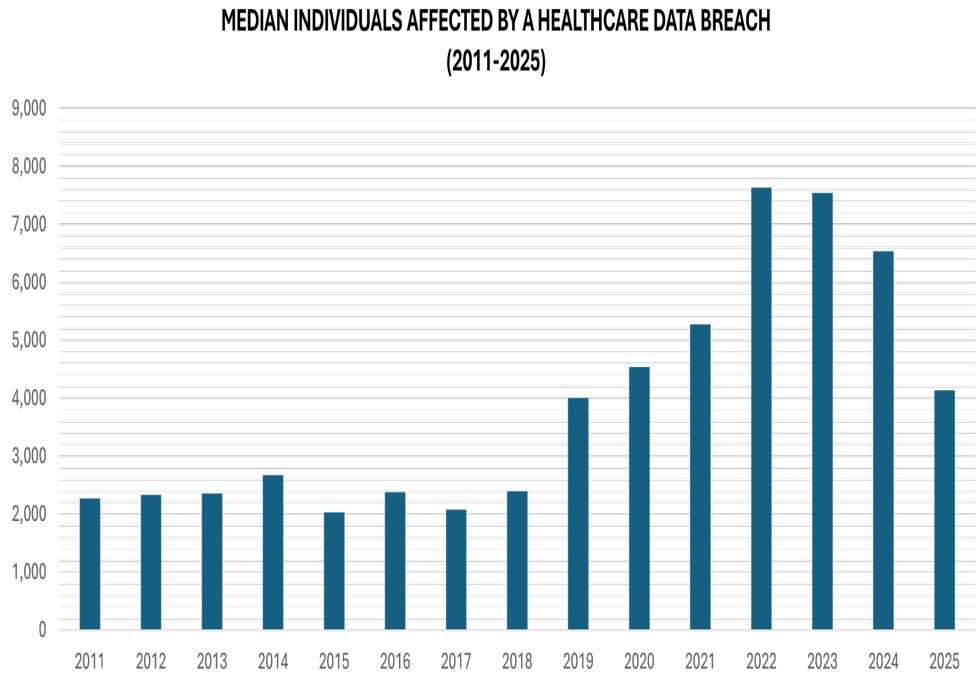

Figure 7. Year-wise distribution of reported healthcare data breach incidents in the United States from 2011 to 2025.

Table 4 categorizes major cybersecurity threats in healthcare environments by attack type, description, and threat origin. It distinguishes between insider and outsider threats to provide a structured view of the healthcare threat landscape. In addition, the table highlights how both technical weaknesses and human factors contribute to healthcare security breaches. By separating threats based on origin and intent, it provides a foundation for designing targeted mitigation and access control strategies.

Table 4. Classification of cyber security threats in healthcare IT systems.

Threat Category	Threat Type	Description	Insider/Outsider
Malware Attacks	Ransomware	Encrypt clinical and administrative data to extort ransom, often disrupting hospital operations and patient care	Outsider
Malware Attacks	Spyware/Trojan	Covertly gather sensitive patient or credential data for unauthorized access or illicit use	Outsider
Network-Based Attacks	Man-in-the-Middle (MitM)	Intercept communications between medical devices, clinicians, and servers, enabling data manipulation or theft	Outsider
Network-Based Attacks	Denial-of-Service (DoS/DDoS)	Flood healthcare networks or services, causing downtime and delaying clinical services	Outsider
Credential-Based Attacks	Brute Force Attacks	Attempt repeated username–password combinations to gain unauthorized system access	Outsider

Table 4. *Cont.*

Threat Category	Threat Type	Description	Insider/Outsider
Credential-Based Attacks	Credential Theft	Use phishing or malware to obtain healthcare staff credentials, enabling unauthorized access	Insider/Outsider
Insider Threats	Malicious Insider	Authorized personnel deliberately misuse access to steal, alter, or disclose sensitive patient data	Insider
Insider Threats	Negligent Insider	Unintentional exposure of data due to poor security practices or policy violations	Insider
System Vulnerabilities	Exploitation of Legacy Systems	Target outdated healthcare systems lacking modern security controls or timely patches	Outsider
Cloud and Data Threats	Data Leakage	Unauthorized disclosure of EHRs due to misconfigurations or weak access control mechanisms	Insider/Outsider

4.8. Vulnerabilities in Healthcare Systems

Common vulnerabilities documented in the literature include:

- Outdated medical devices with un-patched software: Healthcare environments rely heavily on legacy medical devices such as infusion pumps, imaging systems, and patient monitors that often run on outdated operating systems and firmware [76]. Many clinical devices, such as imaging systems, infusion pumps, patient monitors, and laboratory equipment, rely on legacy operating systems that cannot be easily updated due to vendor restrictions, certification requirements, or the risk of disrupting clinical operations. As a result, known vulnerabilities remain unaddressed for extended periods, making these devices attractive targets for cyber attacks. Un-patched systems are particularly susceptible to malware infections, ransomware, and network-based attacks [77], which can compromise device functionality, patient data confidentiality, and overall hospital operations. Furthermore, outdated devices often lack modern security mechanisms such as strong encryption, secure authentication, and intrusion detection capabilities [78]. Given their direct integration into clinical workflows, the exploitation of such vulnerabilities can have severe consequences, including service disruption, data breaches, and risks to patient safety. Addressing this issue requires coordinated efforts involving timely patch management, network segmentation, vendor accountability, and the gradual replacement of legacy medical devices with security-by-design alternatives.

  As a result, un-patched medical devices are commonly associated with ransomware infections, malware propagation, remote code execution, and denial-of-service (DoS) attacks, which can disrupt clinical operations and compromise patient safety.
- Network Mis-configurations: Network mis-configurations represent a critical vulnerability in healthcare systems, arising from improper setup of firewalls, access controls, segmentation policies, and communication protocols [79]. Common issues include overly permissive access rules, exposed services, default credentials, and insufficient network segmentation between clinical, administrative, and IoT device networks. Such weaknesses can enable attackers to move laterally within hospital networks, escalate privileges, and access sensitive patient data. Given the complexity and scale of healthcare IT infrastructures, mis-configurations are often unintentional [80] but can

significantly increase the likelihood and impact of cyber incidents if not systematically identified and corrected. These weaknesses often enable man-in-the-middle (MitM) attacks, lateral movement, privilege escalation, and data ex-filtration, allowing adversaries to intercept sensitive data or compromise multiple systems simultaneously.

- Default system credentials: The continued use of default or weak system credentials remains a critical security weakness in healthcare environments [81]. Many medical devices, network equipment, and healthcare applications are deployed with vendor-provided default usernames and passwords that are rarely changed due to operational oversight or usability concerns. Attackers commonly exploit these credentials through automated scanning and brute-force techniques to gain unauthorized access. Once compromised, default credentials can enable attackers to manipulate device functionality, access sensitive health data, or deploy malicious software [82]. Addressing this vulnerability requires enforcing strong authentication policies, mandatory credential changes, and the adoption of multi-factor authentication where feasible.
  This vulnerability is frequently linked to brute-force attacks, credential stuffing, unauthorized system access, and insider-assisted breaches, ultimately leading to data theft, system manipulation, or ransomware deployment.
- Insecure Firmware: Insecure firmware is a critical vulnerability in healthcare systems, as it operates at a low level and directly controls the behavior of medical devices, network equipment, and embedded systems [83]. When firmware is poorly designed, outdated, unsigned, or lacks integrity verification, attackers can exploit it to gain persistent and often undetectable access to devices. Compromised firmware is particularly dangerous in healthcare because it can survive system reboots and software updates, allowing long-term control over critical devices such as infusion pumps, imaging systems, patient monitors, and IoMT gateways.
  This vulnerability can enable several types of attacks. Firmware without secure boot or cryptographic signing can be modified to install backdoors, leading to advanced persistent threats (APTs) within hospital networks. Attackers may exploit insecure firmware update mechanisms to inject malicious code, resulting in device hijacking or malware propagation across connected systems [84]. In some cases, compromised firmware can be used to manipulate device behavior, causing data integrity attacks (e.g., falsifying patient readings) or denial-of-service (DoS) attacks that disrupt clinical operations. Additionally, insecure firmware may facilitate lateral movement, allowing attackers to pivot from a compromised medical device to other critical healthcare IT infrastructure [12].
- Unencrypted data storage or transmission: The absence of encryption for data at rest or in transit exposes sensitive healthcare information to unauthorized access and interception. Patient records, credentials, and operational data stored or transmitted in plain text can be easily captured by attackers monitoring network traffic or accessing compromised storage systems [85]. This vulnerability directly enables man-in-the-middle (MitM) attacks, eavesdropping, and data leakage, and can also support identity theft and credential harvesting. In clinical systems, unencrypted communications between devices and servers may further allow attackers to alter or inject data, leading to data tampering and potential disruption of medical decision-making processes.
- Legacy systems lacking modern security controls: Legacy healthcare systems often operate on outdated platforms that lack contemporary security mechanisms such as strong encryption, fine-grained access control, continuous monitoring, and compatibility with modern authentication protocols [86]. These systems are frequently retained due to high replacement costs, regulatory constraints, or dependence on specialized clinical workflows. However, their limited security capabilities make them

attractive targets for cyber adversaries. The absence of modern protections increases susceptibility to ransomware attacks, where attackers exploit known weaknesses to encrypt critical clinical data and disrupt healthcare operations [87]. Legacy systems are also vulnerable to unauthorized access and privilege escalation attacks, as they often lack support for multi-factor authentication and robust logging mechanisms [88]. Additionally, outdated protocols and unsupported software components can enable man-in-the-middle attacks, allowing adversaries to intercept or manipulate sensitive healthcare data during transmission. As healthcare infrastructures continue to integrate digital services, the continued reliance on legacy systems significantly amplifies the overall cyber risk profile of healthcare organizations [53].

Research findings show that attackers can exploit weaknesses in device firmware, communication channels, and application layers to infiltrate network infrastructures and gain control of medical operations. Table 5 presents a mapping between key healthcare vulnerabilities (e.g., legacy systems, mis-configurations, weak credentials) and their associated attack types and MITRE ATT&CK tactics.

Table 5. Mapping of healthcare system vulnerabilities to attack types and MITRE ATT&CK tactics.

Healthcare Vulnerability	Associated Attack Types	MITRE ATT&CK Tactics	Healthcare Examples
Outdated medical devices with unpatched software	Ransomware, malware injection, remote code execution	Initial Access, Execution, Persistence	Legacy infusion pumps and imaging systems running outdated operating systems have been exploited during ransomware campaigns such as WannaCry, causing service disruption in hospitals
Network misconfigurations	Man-in-the-middle attacks, lateral movement, data exfiltration	Lateral Movement, Credential Access, Collection	Improperly segmented hospital networks allow attackers to pivot from compromised workstations to electronic health record (EHR) systems, enabling large-scale data breaches
Default system credentials	Unauthorized access, privilege escalation, insider misuse	Initial Access, Privilege Escalation	Medical devices and administrative systems deployed with factory-default passwords have enabled attackers to gain unauthorized access to clinical systems
Insecure firmware	Persistent malware, backdoor installation, stealth attacks	Persistence, Defense Evasion	Unverified firmware updates in medical devices can allow attackers to implant persistent backdoors that survive system reboots, posing long-term risks to patient safety
Unencrypted data storage or transmission	Eavesdropping, data leakage, man-in-the-middle attacks	Collection, Exfiltration	Unencrypted transmission of patient data over internal hospital networks has resulted in exposure of personally identifiable information (PII) and protected health information (PHI)

Table 5. *Cont.*

Healthcare Vulnerability	Associated Attack Types	MITRE ATT&CK Tactics	Healthcare Examples
Legacy systems lacking modern security controls	Exploit-Kit-based attacks, Ransomware, exploitation of known vulnerabilities, denial-of-service	Initial Access, Impact	Older healthcare information systems lacking MFA, endpoint protection, or intrusion detection remain highly vulnerable to modern ransomware and denial-of-service attacks

5. Internet of Things (IoMT) Medical Devices and Equipment

One of the major vulnerabilities in healthcare systems involves Internet of Medical Things (IoMT) medical devices and equipment, which are often poorly protected due to hardware and software limitations. These devices, which include medical imaging equipment, monitoring devices, and other critical equipment, can become tools for attacks and even harm patients if compromised by hackers. Protecting these devices requires specific standards and frequent software updates, which unfortunately are still not fully implemented in many healthcare facilities.

The software used in healthcare information systems, especially outdated or poorly updated software, is highly susceptible to security vulnerabilities that can be exploited by attackers [89]. The lack of effective update management and security patching policies increases this risk and makes systems vulnerable to a variety of malicious attacks, including network intrusion and malicious code execution. Therefore, implementing regular update processes and closely monitoring the security status of software are inevitable necessities.

The Internet of Medical Things (IoMT) has emerged as a transformative paradigm in modern healthcare by enabling interconnected medical devices, wearable and implantable sensors, gateways, cloud platforms, and healthcare information systems to deliver real-time monitoring and personalized care. Despite these benefits, the increased connectivity and heterogeneity of IoMT ecosystems significantly expand the attack surface, making cyber security a critical challenge for healthcare systems [90].

As shown in Figure 8, smart healthcare environments integrate mobile health apps, patient monitoring devices, emergency response services, and hospital information systems to support continuous care delivery. IoMT architectures typically consist of resource-constrained medical devices, wireless communication technologies (e.g., Bluetooth, Wi-Fi, cellular networks), edge gateways, and cloud-based analytics platforms. Each architectural layer introduces unique security vulnerabilities. According to Papaioannou et al., IoMT devices often lack strong computational capabilities and robust built-in security mechanisms, rendering them vulnerable to both internal and external cyber threats [30]. These limitations are further aggravated by long device life-cycles and infrequent firmware updates.

Cybersecurity threats in IoMT span multiple layers of the system. Device-level threats include physical tampering, firmware manipulation, and malware injection, which can directly compromise device functionality and patient safety. At the network level, attacks such as eavesdropping, spoofing, man-in-the-middle, replay, and denial-of-service attacks threaten the confidentiality, integrity, and availability of medical data transmissions [30]. System- and application-level threats target electronic health records, hospital networks, and cloud infrastructures, often resulting in data breaches and ransomware incidents [90].

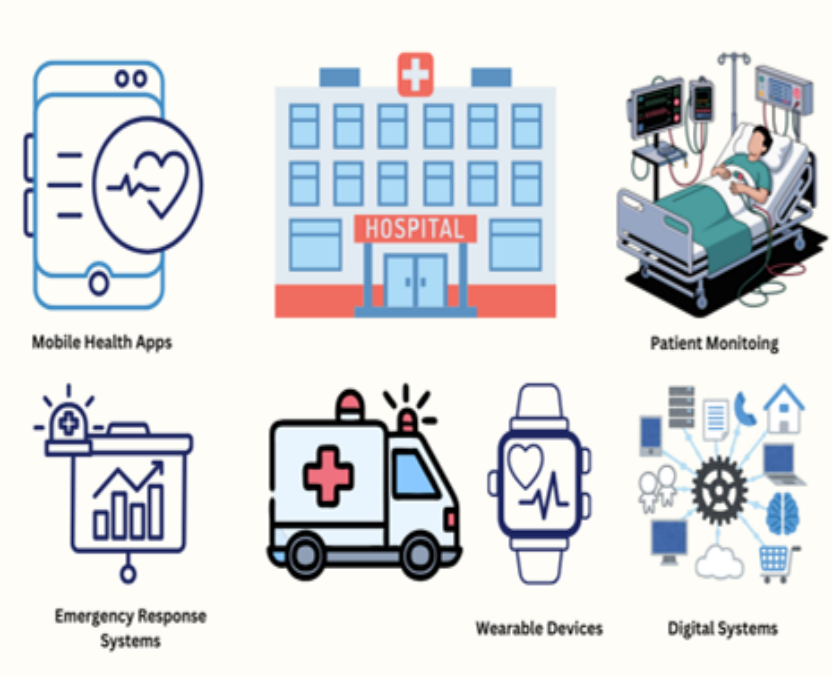

Figure 8. Internet of Medical Things (IoMT).

Unlike traditional IT systems, cyberattacks on IoMT environments can have severe physical consequences. Compromised medical devices may deliver incorrect dosages, delay critical treatment, or malfunction during life-support operations. Recent studies emphasize that healthcare systems constitute a form of critical infrastructure where cyber incidents can escalate into life-threatening situations [91]. This tight coupling between cyber systems and physical patient outcomes distinguishes IoMT security from conventional information security domains.

Privacy and data protection are also major concerns in IoMT ecosystems. Continuous collection of sensitive physiological and behavioral data exposes patients to risks of unauthorized access, identity theft, and data misuse. Medical data are considered highly valuable in underground markets, making healthcare organizations attractive targets for cybercriminals [30]. Although regulatory frameworks such as HIPAA and GDPR impose strict data protection requirements, enforcing compliance remains challenging due to interoperability requirements and cross-border data exchange.

Recent research highlights that conventional perimeter-based security mechanisms are insufficient for IoMT environments. Instead, a layered and security-by-design approach is required, incorporating lightweight cryptographic techniques, continuous monitoring, intrusion detection, and adaptive risk management frameworks [92]. Such approaches aim to balance strong security guarantees with the limited computational and energy resources of medical devices.

Recent research indicates that conventional perimeter-based security mechanisms are insufficient for the dynamic and resource-constrained Internet of Medical Things (IoMT) environment. Consequently, existing studies advocate a layered, security-by-design approach that integrates lightweight cryptography with continuous monitoring, intrusion detection, and adaptive risk-management frameworks. To address computational and energy limitations of medical devices, several lightweight cryptographic techniques have been proposed, including hyperchaotic map-based encryption combined with Fibonacci Q-matrix operations, logistic parity-based chaotic encryption, and combined transformation and expansion (CTE) schemes for efficient data confidentiality in IoMT systems. In parallel, proxy re-encryption mechanisms leveraging elliptic-curve cryptography (ECC), such

as Ed25519- and X25519-based lightweight proxy re-encryption, have been employed to enable secure and flexible data sharing with low computational overhead [69]. Furthermore, identity-based proxy re-encryption (IB-PRE) schemes have been explored to reduce key-management complexity while achieving lower encryption, decryption, and energy consumption compared to traditional public-key approaches [71]. At the network level, ECC-based lightweight authentication and encryption integrated into cross-layer secure routing protocols have demonstrated improved energy efficiency and reduced cryptographic overhead in IoMT-enabled healthcare networks [73]. Collectively, these approaches aim to balance strong security guarantees with the stringent computational, memory, and energy constraints inherent to medical and wearable devices.

5.1. Zero-Trust Brokerage Between IoMT Devices and EHR Systems

In healthcare systems and Internet of Medical Things (IoMT) environments, zero-trust architecture (ZTA) works by removing the assumption that any user, device, or network segment can be trusted by default. Instead of relying on a secure perimeter, access decisions are made dynamically based on identity, context, and observed behavior. Clinicians, administrative users, and connected medical devices must authenticate each time they request access, and permissions are limited strictly to what is required for their role. Medical devices are treated as individual entities with their own identities and are continuously assessed for compliance, such as firmware status or abnormal communication patterns. Hospital networks are also divided into smaller, isolated segments, ensuring that a compromised device or account cannot freely move across systems. Data exchanges are protected using encrypted communication channels, while ongoing monitoring helps identify unusual activity that may indicate insider misuse or device compromise. Through these combined measures, ZTA strengthens security in healthcare and IoMT systems by reducing attack surfaces and limiting the impact of both internal and external threats.

Recent empirical investigations have demonstrated the practical effectiveness of zero-trust architecture (ZTA) within healthcare environments. For example, real-world deployments in large healthcare institutions have reported notable reductions in security incidents following the adoption of micro-segmented network designs, with some organizations observing breach reductions of approximately 40% after implementation [93]. Broader longitudinal analyses across multiple U.S. hospitals further indicate that ZTA significantly reduces ransomware dwell time, decreasing persistence periods from several weeks to only a few days by enforcing continuous verification and least-privilege access controls [94]. Evidence from Internet of Medical Things (IoMT) deployments also supports these findings. Large-scale implementations involving thousands of connected medical devices have achieved high compliance levels and demonstrated increased resistance to phishing and credential-based attacks through behavior-aware authentication mechanisms [95]. Federated learning pilots conducted across multi-hospital consortia have demonstrated up to an 85% improvement in threat-detection performance, while enabling collaborative model training without direct exposure of sensitive patient data [96]. Collectively, these empirical outcomes suggest that ZTA not only strengthens healthcare cybersecurity posture but also delivers measurable economic benefits by reducing the financial impact of major security breaches.

Figure 9 illustrates a zero-trust architecture governing secure interactions between Internet of Medical Things (IoMT) devices and electronic health record (EHR) systems. In this architecture, IoMT assets, user devices, and applications are treated as untrusted by default and must undergo continuous authentication and authorization before accessing enterprise healthcare resources. The control plane comprises identity and access management, data and endpoint security services, and policy decision components (policy

engine and policy administrator) that dynamically evaluate trust based on device posture, user identity, and contextual attributes. The data plane enforces these decisions through policy enforcement points, regulating access to EHR databases and clinical applications in accordance with least-privilege principles. This design ensures continuous verification, minimizes lateral movement, and protects sensitive patient data throughout IoMT–EHR communication.

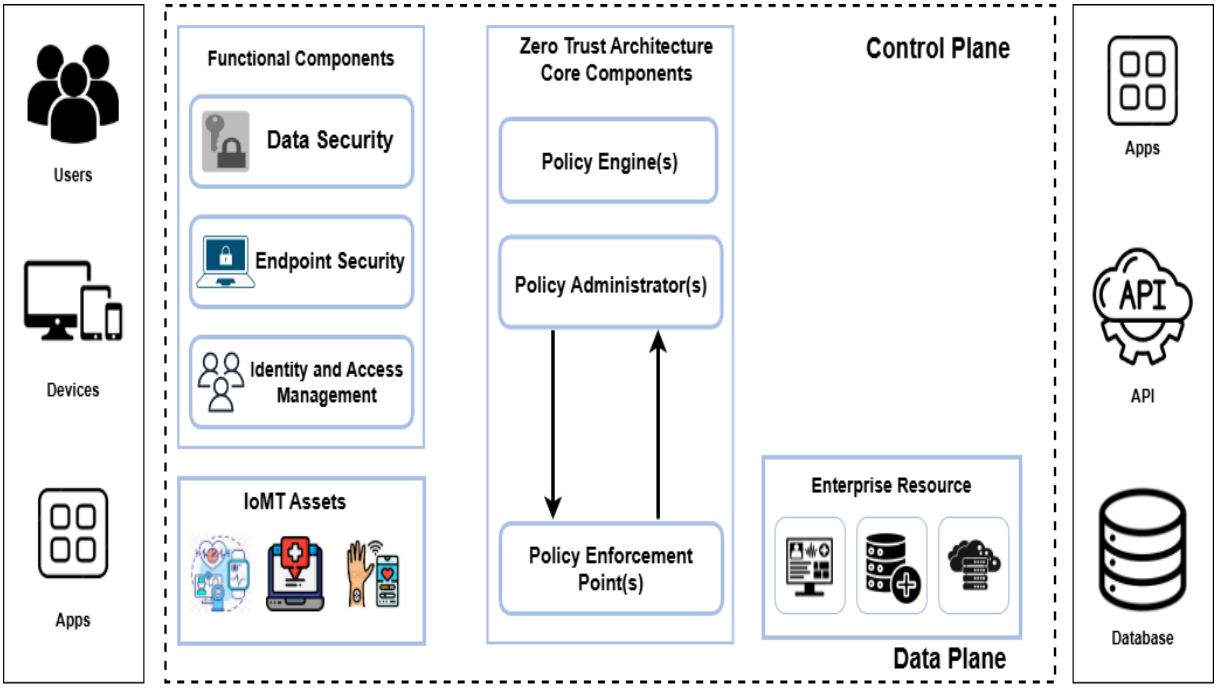

Figure 9. Zero-trust architecture between IoMT and EHR.

Overall, ensuring cybersecurity in IoMT systems requires a holistic strategy that integrates technical safeguards, organizational policies, and regulatory compliance. As IoMT adoption continues to grow, future research must focus on resilient architectures and proactive defense mechanisms to safeguard patient safety, privacy, and trust in digital healthcare systems [90,92].

5.2. Research Gaps and Open Challenges in IoMT Cyber Security

Despite significant progress in identifying threats and proposing countermeasures, cyber security in the Internet of Medical Things (IoMT) remains an open and evolving research area. Existing studies largely focus on threat classification and conceptual security frameworks, while practical, scalable, and clinically deployable solutions are still limited [30,92].

1. Resource Constraints and Lightweight Security: One of the fundamental challenges in IoMT security is the severe resource limitation of medical devices, including constrained processing power, memory, and battery life. Many conventional cryptographic and intrusion detection mechanisms designed for traditional IT systems are unsuitable for implantable or wearable medical devices [30]. Although lightweight cryptographic schemes have been proposed, there is still a lack of standardized, clinically validated solutions that balance security, energy efficiency, and real-time responsiveness.
2. Security versus Safety Trade-offs: A critical research gap lies in the interaction between cyber security and patient safety. Security mechanisms such as frequent authentication, encryption, or firmware updates may introduce latency or operational disruptions

that are unacceptable in life-critical medical applications. Current literature often treats security and safety as separate concerns, whereas IoMT systems require integrated frameworks that explicitly model and manage their inter-dependencies [92]. Establishing formal methods to evaluate the safety impact of security controls remains an open challenge.

3. Lack of Real-World Validation and Deployment Studies: Most existing IoMT security solutions are evaluated through simulations or small-scale testbeds. There is a notable lack of real-world deployment studies demonstrating long-term effectiveness, usability, and resilience in clinical environments [90]. Healthcare organizations operate under strict regulatory, operational, and financial constraints, which are often overlooked in academic research. Bridging the gap between laboratory research and hospital-scale implementation is essential.
4. Heterogeneity and Interoperability Challenges: IoMT ecosystems are inherently heterogeneous, comprising devices from multiple vendors, legacy medical equipment, diverse communication protocols, and cloud services. This heterogeneity complicates the enforcement of uniform security policies and consistent patch management [30]. Interoperability requirements often force security compromises, creating weak links that attackers can exploit. Future research must address secure interoperability without sacrificing compatibility or clinical usability.
5. Limited Incident Reporting and Threat Intelligence Sharing: Another major gap is the lack of transparent incident reporting and shared threat intelligence in the healthcare sector. Cyber incidents involving medical devices are often under-reported due to reputational concerns and regulatory implications [90]. This limits the availability of real-world attack data, hindering the development of accurate threat models and evidence-based defense mechanisms.
6. Regulatory and Compliance Challenges: While regulatory bodies such as the FDA and European MDR emphasize cyber security, regulations often lag behind rapidly evolving threats. Existing standards provide high-level guidance but lack detailed technical specifications for secure-by-design IoMT systems [92]. Moreover, global variations in regulatory requirements complicate cross-border IoMT deployments and data sharing, highlighting the need for harmonized cyber security standards.
7. Emerging Threats and Future Technologies: The increasing integration of AI, cloud computing, and edge intelligence into IoMT introduces new attack vectors, including data poisoning, model inversion, and adversarial learning attacks. Current IoMT security literature provides limited coverage of these emerging threats [92]. As healthcare systems move toward data-driven and autonomous decision-making, securing both data and learning processes becomes a critical research priority.
8. Need for Proactive and Adaptive Security Frameworks: Most existing approaches focus on reactive defenses, such as detecting known attacks or patching vulnerabilities after discovery. There is a growing need for proactive, adaptive, and risk-aware security frameworks capable of anticipating threats and responding dynamically to changing attack surfaces [91]. Incorporating continuous monitoring, threat intelligence, and adaptive defense mechanisms remains an open research challenge.

6. Impact of Cyber Threats on Patient Safety and Operations

Cyber attacks are not limited to financial or privacy risks; they may directly disrupt clinical operations, delay treatment, and affect diagnosis accuracy. Studies report that healthcare attacks can compromise medical sensors, modify patient data, manipulate drug dosage settings, or disable diagnostic equipment. Cyber security breaches in healthcare have severe consequences for patient data confidentiality, integrity, and availability. Unau-

thorized access to electronic health records (EHRs) can expose highly sensitive information, including medical histories, diagnoses, insurance details, and personal identifiers, leading to identity theft, insurance fraud, and long-term privacy violations [97]. Data manipulation or loss resulting from cyber attacks, such as ransomware or insider misuse, can compromise data integrity, potentially causing clinical errors, delayed treatments, or incorrect medical decisions that directly threaten patient safety. Moreover, large-scale data breaches undermine patient trust in healthcare providers and digital health technologies, which may reduce patient engagement and willingness to share accurate information [98].

Recent industry evidence further quantifies the substantial economic impact of cybersecurity breaches in healthcare systems. According to the Cost of a Data Breach Report 2025, published by the Ponemon Institute in collaboration with IBM, the global average cost of a data breach reached USD 4.44 million, marking a slight decline compared to previous years due to faster breach detection enabled by AI-driven security tools. Despite this global reduction, the healthcare sector continues to be the most financially affected industry, recording an average breach cost of USD 7.42 million, the highest among all sectors for the twelfth consecutive year. In addition, the average cost per compromised record remains high, with sensitive personal data such as customer and patient personally identifiable information (PII) costing approximately USD 160–166 per record, depending on data type [99].

The disproportionately high breach costs in healthcare are primarily attributed to extended breach life-cycles, with healthcare incidents taking an average of 279 days to identify and contain, significantly longer than the global average. Additional cost drivers include regulatory fines, which affected nearly one-third of breached organizations, operational disruptions to critical clinical services, and extensive post-breach response efforts, such as forensic investigations, patient notification, credit monitoring, and long-term infrastructure remediation.

These findings demonstrate that cyber security breaches in healthcare are not merely technical failures or privacy violations but represent a persistent economic and operational risk. Consequently, quantifying breach costs reinforces the urgency of deploying robust cyber security architectures, privacy-preserving data management frameworks, and proactive threat detection mechanisms, particularly in data-intensive and mission-critical healthcare environments [99].

From an organizational perspective, breaches involving patient data often result in substantial financial losses, regulatory penalties under frameworks such as HIPAA and GDPR, legal liabilities, and long-term reputational damage. However, despite their shared objective of protecting sensitive health information, HIPAA and GDPR differ considerably in their technical and operational requirements, including breach-notification timelines, encryption expectations, and patient or data-subject rights. To clarify these distinctions and their implications for healthcare cyber security system design, a comparative overview of HIPAA and GDPR is provided in Table 6.

Recent industry reports provide concrete evidence of the substantial economic consequences associated with cyber security breaches in healthcare systems. According to the 2023 Cost of a Data Breach report published by the Ponemon Institute in collaboration with IBM, the average cost per compromised record across all industries is approximately USD 165. Notably, the healthcare sector continues to incur the highest breach-related costs, with an average total cost of USD 10.93 million per incident, significantly exceeding other critical sectors such as finance and energy.

These elevated costs stem from several healthcare-specific factors. First, healthcare organizations typically experience longer breach identification and containment times, often exceeding 300 days, due to complex legacy systems, heterogeneous medical devices,

and fragmented IT infrastructures. Second, breaches frequently result in regulatory and legal penalties, driven by strict compliance requirements under healthcare data-protection regulations. Third, cyber security incidents can directly disrupt clinical operations, leading to delayed treatments, diversion of emergency services, and temporary system shutdowns, which further amplify financial losses and reputational damage. Finally, extensive post-breach remediation efforts, including system recovery, forensic investigations, patient notification, credit monitoring, and long-term security upgrades, contribute significantly to the overall economic impact.

Table 6. Technical and operational comparisons of HIPAA and GDPR in healthcare data protection.

Aspect	HIPAA	GDPR
Scope of Applicability	U.S.-based healthcare providers, insurers, and business associates	All organizations processing personal data of EU residents
Type of Data Covered	Protected Health Information (PHI)	Personal data and special category data, including health data
Breach Notification Window	Within 60 days of breach discovery	Within 72 h of breach discovery
Encryption Requirement	Addressable safeguard; recommended but not mandatory	Explicitly encouraged through encryption and pseudonymization
Access Control	Role-based access controls required	Principle of least privilege and access minimization
Data Minimization	Not explicitly defined	Explicitly mandated as a core principle
Patient/Data Subject Rights	Right to access and amend records	Rights to access, rectification, erasure, and data portability
Cross-Border Data Transfer	No explicit restrictions	Strict controls requiring adequacy decisions or safeguards
Penalties for Non-Compliance	Civil and criminal penalties with capped fines	Fines up to EUR 20 million or 4% of global annual turnover
Privacy by Design	Not explicitly required	Explicitly mandated by regulation

Cybersecurity data breaches involving patient data have far-reaching consequences for individuals, healthcare organizations, and the broader health ecosystem. When electronic health records (EHRs) are compromised, highly sensitive information such as medical histories, diagnoses, insurance details, and personal identifiers may be exposed [100]. Unlike financial data, medical data cannot be easily changed, making it particularly valuable for identity theft, insurance fraud, and long-term misuse. Patients affected by data breaches often experience loss of privacy, emotional distress, and a decline in trust toward healthcare providers, which can discourage them from fully disclosing information necessary for effective medical care.

Beyond patient-level harm, breaches significantly disrupt healthcare operations and clinical workflows [101]. Cyber attacks such as ransomware can render hospital information systems unavailable, forcing delays or cancellations of appointments, diagnostic procedures, and even critical treatments. In extreme cases, system outages may require providers to revert to manual processes, increasing the likelihood of medical errors and compromising patient safety. Studies have shown that cyber incidents in healthcare are associated with increased mortality rates and adverse clinical outcomes, underscoring that cyber security is not only an IT concern but also a patient safety issue.

From an organizational perspective, data breaches impose substantial financial and legal burdens on healthcare institutions. Costs arise from incident response, forensic

investigations, system restoration, regulatory penalties, and potential litigation. Healthcare organizations are also subject to strict data protection regulations, such as HIPAA, and non-compliance following a breach can result in severe fines and reputational damage. Repeated or high-profile incidents can erode public confidence, affect partnerships, and hinder the adoption of digital health technologies. Consequently, safeguarding patient data is essential not only for privacy and compliance but also for maintaining continuity of care and long-term organizational resilience.

Moreover, large-scale breaches contribute to systemic risks across the healthcare sector. Aggregated stolen health data can be exploited to target future attacks, including social engineering campaigns against patients or follow-up intrusions into interconnected healthcare networks [102]. As healthcare systems become increasingly data-driven and interconnected through cloud services, tele-medicine, and IoMT devices, the impact of a single breach can cascade across multiple stakeholders. This highlights the critical need for proactive cyber security strategies that integrate technical controls, governance, and human-centric defenses to protect patient data and preserve trust in digital healthcare systems [103].

7. Data Privacy Challenges in Healthcare

Healthcare environments manage extremely sensitive information, including medical histories, diagnostic data, personal identifiers, financial information, treatment records, and genetic profiles [104]. This makes patient data a high-value asset that is difficult to replace or revoke once compromised [105]. Unlike leaked passwords or credit information, medical data remains permanently associated with the individual and can be exploited for identity theft, insurance fraud, or social engineering over long periods of time.

Privacy risks often originate from weak security configurations, insecure device communication channels, or insufficient protection of cloud-based data stores. IoMT systems transmit information across wireless and networked endpoints, meaning that a breach at any point in the communication chain, such as un-encrypted traffic or insecure gateway devices, may result in unauthorized disclosure of patient information [106].

Figure 10 summarizes the major challenges in protecting patient privacy, including data breaches and cyber threats, insider threats and human errors, inadequate security training, and security weaknesses in third-party services.

Data privacy concerns are also magnified by the complex and fragmented nature of healthcare networks [107]. Hospitals frequently operate mixtures of legacy medical systems, third-party vendor platforms, and modern IoT devices, each governed by different security capabilities and update cycles. This lack of standardization makes maintaining consistent privacy controls across the environment difficult. Healthcare organizations may further struggle with limited IT staffing, inconsistent monitoring capabilities, and difficulty detecting real-time data misuse or system compromise.

As a result, privacy breaches often occur not only due to external attacks but also through unauthorized internal access, incomplete data governance, poor logging practices, or mis-configurations that expose patient data unintentionally. Ensuring robust privacy protections, therefore, requires ongoing governance, continuous monitoring, regular security updates, and improved interoperability among healthcare applications and devices [108].

Cryptographic techniques for protecting healthcare data typically rely on encryption mechanisms such as public-key encryption (PKE) and symmetric-key encryption (SKE) [109]. In addition to these conventional approaches, advanced cryptographic primitives have been proposed to enhance data privacy in healthcare environments. These include identity-based encryption (IBE), hierarchical or predicate encryption (HPE), and

fully homomorphic encryption (FHE), which enable fine-grained access control and secure computation over encrypted health data.

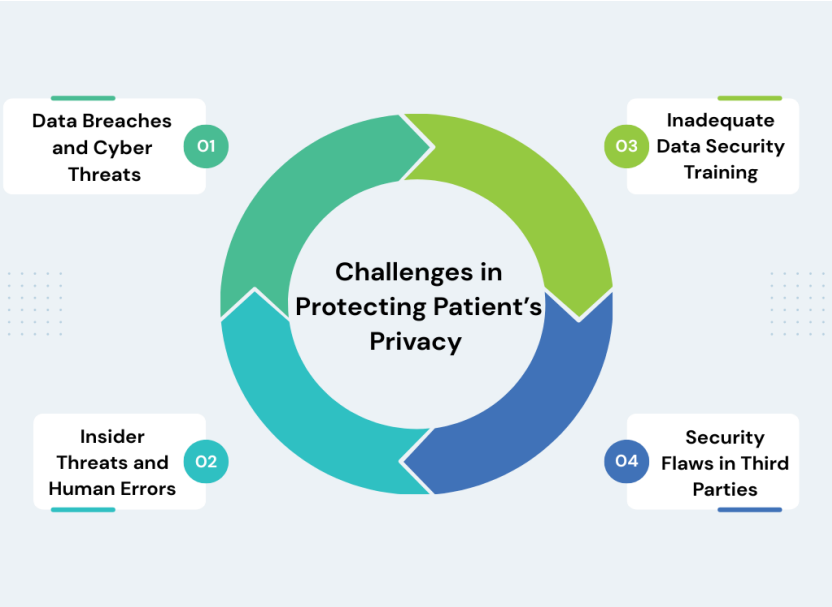

Figure 10. Challenges in protecting patient data privacy.

Multiple consensus mechanisms have been proposed as alternatives to proof of work (PoW), aiming to improve energy efficiency and system robustness. Among these, practical Byzantine fault tolerance (PBFT) is particularly well suited for healthcare blockchain applications due to its low latency and deterministic performance [110]. PBFT can tolerate up to one-third Byzantine faults in a network consisting of 3f+1 nodes and operates through five phases: request, pre-prepare, prepare, commit, and reply. The protocol assumes a permissioned environment where participating entities are known in advance, making it appropriate for healthcare systems that require controlled access and fast transaction confirmation.

Sharma et al. [111] proposed a blockchain-enabled distributed application for IoT-based healthcare systems to securely generate, store, and manage medical certificates. The framework leverages smart contracts and a decentralized ledger to mitigate common security threats such as data tampering, unauthorized access, and certificate forgery. By eliminating centralized cloud dependence, the system improves transparency, integrity, and privacy of healthcare records. Experimental evaluations using Ethereum tools demonstrate reduced latency and improved throughput compared to existing solutions, highlighting the feasibility of blockchain for secure IoT healthcare data management.

Li et al. [112] introduced ADDETECTOR, a federated learning-based smart healthcare framework for early Alzheimer's disease detection using IoT voice data. The system employs a three-layer architecture and integrates federated learning, differential privacy, and cryptographic aggregation to prevent data leakage at data, feature, and model levels. By retaining raw data at user devices and sharing only protected model updates, the framework ensures strong privacy guarantees. Experimental results show that ADDETECTOR achieves competitive detection accuracy with minimal computational overhead, demonstrating the effectiveness of federated learning for privacy-preserving healthcare analytics.

Researchers have also proposed a blockchain-based framework for secure and privacy-preserving EMR exchange and sharing in open healthcare networks [113]. The system integrates dynamic access control via smart contracts with local differential privacy to achieve fine-grained, attribute-level privacy protection. Sensitive EMR attributes were selectively randomized based on requester roles, enabling personalized privacy control

while maintaining data utility. Prototype implementation and large-scale evaluation using real-world EMRs confirmed that the framework supports reliable, traceable, and privacy-aware medical data transactions.

The study presented a secure and intelligent healthcare monitoring framework that integrates Internet of Medical Things (IoMT) data with advanced machine learning techniques to enhance cyberattack and anomaly detection. The authors employed recursive feature elimination (RFE) combined with logistic regression and extreme gradient boosting to identify the most relevant security features, followed by a multilayer perceptron (MLP) classifier optimized using hyperparameter tuning and cross-validation. The proposed model was evaluated on multiple real-world healthcare and IoMT cybersecurity datasets, achieving very high detection accuracy across diverse operating systems, networks, and medical telemetry data. The results demonstrated the effectiveness of feature optimization and deep learning for strengthening cybersecurity in IoMT-enabled healthcare environments, particularly against sophisticated and evolving cyber threats [114,115].

8. Future Directions

Despite significant progress in securing healthcare systems, the evolving threat landscape and increasing reliance on interconnected technologies continue to expose critical security and privacy gaps. Future research should therefore focus on developing holistic, adaptive, and context-aware security frameworks that can respond to both technical and organizational challenges in healthcare environments.

One important direction lies in advancing zero-trust security models tailored specifically for healthcare and IoMT ecosystems. While zero trust has gained attention, its practical deployment across heterogeneous medical devices, legacy hospital systems, and cloud-based EHR platforms remains underexplored. Future work should investigate lightweight trust-brokering mechanisms, continuous risk assessment, and interoperability-aware policy enforcement that can operate under strict latency and resource constraints without disrupting clinical workflows.

Another promising research avenue involves the integration of privacy-preserving intelligence, particularly federated learning and secure multi-party computation, for threat detection and anomaly analysis. Although these approaches reduce raw data sharing, challenges related to data heterogeneity, communication overhead, model poisoning, and performance degradation persist. Future studies should focus on robust federated learning frameworks that balance detection accuracy, privacy guarantees, and real-world deployability in healthcare settings.

The growing adoption of IoMT devices and remote healthcare services also calls for deeper investigation into device-centric security. Research is needed on secure firmware update mechanisms, device attestation, and long-term life-cycle management of implantable and wearable medical devices. In addition, standardized security benchmarks and datasets for IoMT threat modeling would significantly improve reproducibility and comparative evaluation across studies.

From a data privacy perspective, future research should move beyond compliance-driven protection toward patient-centric privacy models. This includes dynamic consent management, fine-grained access control, and transparent auditability of data usage across healthcare stakeholders. Exploring hybrid approaches that combine cryptographic techniques, blockchain-based trust, and policy-driven governance may offer stronger assurances of accountability and data integrity.

Finally, there is a need for cross-disciplinary and real-world validation of proposed security solutions. Many existing studies remain conceptual or evaluated in controlled environments. Future work should emphasize deployment-oriented research, incorporating

clinical constraints, regulatory requirements, and human factors. Collaboration between cyber security researchers, healthcare professionals, and policymakers will be essential to ensure that future solutions are not only technically sound but also practical, ethical, and sustainable.

9. Conclusions

This review has examined the evolving landscape of cyber security and data privacy strategies in healthcare IT systems, highlighting the unique challenges posed by digital transformation, interconnected medical devices, cloud-based services, and data-intensive clinical workflows. Healthcare organizations remain highly vulnerable to a wide range of threats, including ransomware, network intrusions, insider misuse, and data leakage, largely due to legacy systems, mis-configurations, and human-related factors. The surveyed literature demonstrates that effective protection of patient data requires a multi-layered defense approach that integrates technical controls (such as access control, encryption, intrusion detection, and secure architectures), organizational measures (including policies, training, and insider threat management), and emerging technologies like blockchain, machine learning, and secure IoT frameworks. Despite notable progress, gaps remain in scalability, interoperability, and real-world deployment of advanced security solutions, particularly in resource-constrained healthcare environments. Future research should focus on developing adaptive, privacy-preserving, and regulation-compliant security mechanisms that can evolve alongside healthcare technologies, ensuring both patient safety and trust in digital healthcare systems.

Author Contributions: Conceptualization, R.Q. and I.K.; methodology, R.Q.; software, R.Q.; validation, I.K.; formal analysis, R.Q.; investigation, R.Q.; resources, R.Q. and I.K.; data curation, R.Q.; writing—original draft, R.Q.; writing—review and editing, I.K.; visualization, R.Q.; supervision, I.K.; project administration, I.K.; funding acquisition, I.K. All authors have read and agreed to the published version of the manuscript.

Funding: The results were supported by the "Regional Innovation System & Education (RISE)" through the Ulsan RISE Center, funded by the Ministry of Education (MOE) and the Ulsan Metropolitan City, Republic of Korea (2025-RISE-07-001).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shen, Y.; Yu, J.; Zhou, J.; Hu, G. Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: Comprehensive review. *J. Med. Internet Res.* **2025**, *27*, e59024. [CrossRef]
2. Eappen, P.; Vajjhala, N.R. (Eds.) *Healthcare Informatics Innovation Post COVID-19 Pandemic*, 1st ed.; Auerbach Publications (Taylor & Francis): New York, NY, USA, 2025. [CrossRef]
3. Ogbodo, D.C.; Awan, I.-U.; Cullen, A.; Zahrah, F. From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection. *Electronics* **2025**, *14*, 2629. [CrossRef]
4. Balogun, A.Y. Strengthening compliance with data privacy regulations in US healthcare cybersecurity. *Asian J. Res. Comput. Sci.* **2025**, *18*, 154–173. [CrossRef]
5. Huang, Z.-K.; Zeng, N.-C.; Zhang, D.-M.; Argyroudis, S.; Mitoulis, S.-A. Resilience models for tunnels recovery after earthquakes. *Engineering* **2025**, *6*, 28. [CrossRef]
6. Imoisi, S.E.; Ottah, I.O. Data security, confidentiality in healthcare management in Nigeria: Need for compliance with health information law. *Med. Health Sci. Eur. J.* **2025**, *9*, 1–30.

7. Ewoh, P.; Vartiainen, T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review. *J. Med. Internet Res.* **2024**, *26*, e46904. [CrossRef] [PubMed]
8. Fuentes, M.R. Cybercrime and other threats faced by the healthcare industry. *Trend Micro* **2017**, *5566*. Available online: http://sitemaps.b51.nl/sites/default/files/pdf/wp-cybercrime-%26-other-threats-faced-by-the-healthcare-industry.pdf (accessed on 27 January 2026).
9. Ahmed, S.; Ahmed, I.; Kamruzzaman, M.; Saha, R. Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies and Future Trend. *Glob. Mainstream J. Innov. Eng. Emerg. Technol.* **2022**, *1*, 36–61.
10. Tiwo, O.J.; Adesokan-Imran, T.O.; Babarinde, D.C.; Oyekunle, S.M.; Olutimehin, A.T.; Olaniyi, O.O. Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data. *Asian J. Res. Comput. Sci.* **2025**, *18*, 187–208. [CrossRef]
11. Alharbe, N.; Almalki, M. IoT-enabled healthcare transformation leveraging deep learning for advanced patient monitoring and diagnosis. *Multimed. Tools Appl.* **2025**, *84*, 21331–21344. [CrossRef]
12. Katsuya, R.; Liu, X. Policy and management implications of firmware vulnerabilities in medical IoT devices: A multi-case analysis. *J. Sci. Technol. Policy Manag.* **2025**, *Epub ahead of printing*. [CrossRef]
13. Alserhani, F. Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical System Design. *Sensors* **2025**, *25*, 4720. [CrossRef]
14. Snigdha, E.Z.; Jalil, M.S.; Dahwal, F.M.; Saeed, M.; Mehedy, M.T.J.; Hasan, S.K.; Al Mamun, A.; Khan, M.D.N. Cybersecurity in Healthcare IT Systems: Business Risk Management and Data Privacy Strategies. *Am. J. Eng. Technol.* **2025**, *7*, 163–184. [CrossRef]
15. Kadam, D.; Budaragade, A.P.; Salunkhe, U.; Gurav, U.P.; Patil, A. Internet of Medical Things: Architecture, Trends, Challenges and the Evolution Towards IoMT 5.0. *Comput. Netw. Commun.* **2025**, 148–163. [CrossRef]
16. Ezeanyim, O.C.; Nwabunwanne, E.C.; Igbokwe, N.C.; Nwamekwe, C.O. Patient Flow and Service Efficiency in Public Hospitals. *J. Health Indones.* **2025**, *3*, 104–124. [CrossRef]
17. ElSayed, Z.; Abdelgawad, A.; Elsayed, N. Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions. *arXiv* **2025**, arXiv:2501.11250. [CrossRef]
18. Dalal, A. Addressing Challenges in Cybersecurity Implementation Across Diverse Industrial and Organizational Sectors. *SSRN* **2025**, SSRN 5268082. [CrossRef]
19. Shojaei, P.; Vlahu-Gjorgievska, E.; Chow, Y.-W. Security and privacy of technologies in health information systems: A systematic literature review. *Computers* **2024**, *13*, 41. [CrossRef]
20. Jarkas, O.; Ko, R.; Dong, N.; Mahmud, R. A Container Security Survey: Exploits, Attacks and Defenses. *ACM Comput. Surv.* **2025**, *57*, 1–36. [CrossRef]
21. Aldosari, B. Cybersecurity in Healthcare: New Threat to Patient Safety. *Cureus* **2025**, *17*, e83614. [CrossRef]
22. Erukayenure, O.; Bashir, H.A.; Adekunbi, A.; Abere, S.E.; Okpan, O.; Guwa, A.A. Human factor vulnerabilities in healthcare cybersecurity: Mitigating insider threats in medical facilities. *Int. J. Sci. Res. Arch.* **2025**, *17*, 024–031. [CrossRef]
23. Safavi, S. A Lightweight AI Model for Detecting Insider Threats in Hospital Networks. *ResearchGate Preprint* **2024**. [CrossRef]
24. Newman, K.D.D. Advanced Privacy-Preserving Decentralized Federated Learning for Insider Threat Detection in Collaborative Healthcare Institutions. Ph.D. Thesis, The George Washington University, Washington, DC, USA, 2025.
25. Lee, I. Analysis of insider threats in the healthcare industry: A text mining approach. *Information* **2022**, *13*, 404. [CrossRef]
26. Ijaz, N.; Hasan, M.N.; Koo, I. Few-Shot Transfer Learning-Based Fault Classification in Wireless Sensor Networks. *IEEE Access* **2025**, *13*, 55017–55033. [CrossRef]
27. Velagala, L.P.; Hossain, G. Analyzing insider threats and human factors in healthcare 5.0. In Proceedings of the 2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET), Boca Raton, FL, USA, 4–6 December 2023; pp. 95–100.
28. Deep, G.; Sidhu, J.; Mohana, R. Insider threat prevention in distributed database as a service cloud environment. *Comput. Ind. Eng.* **2022**, *169*, 108278. [CrossRef]
29. Mohammed, M.A.; Lakhan, A.; Zebari, D.A.; Abdulkareem, K.H.; Nedoma, J.; Martinek, R.; Tariq, U.; Alhaisoni, M.; Tiwari, P. Adaptive secure malware efficient machine learning algorithm for healthcare data. *CAAI Trans. Intell. Technol.* **2023**. [CrossRef]
30. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A survey on security threats and countermeasures in internet of medical things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
31. Bhosale, K.S.; Nenova, M.; Iliev, G. A study of cyber attacks: In the healthcare sector. In Proceedings of the 2021 Sixth Junior Conference on Lighting, Gabrovo, Bulgaria, 23–25 September 2021; pp. 1–6.
32. Ray, S.; Mishra, K.N.; Dutta, S. Detection and prevention of DDoS attacks on M-healthcare sensitive data: A novel approach. *Int. J. Inf. Technol.* **2022**, *14*, 1333–1341. [CrossRef]
33. Ijaz, N.; Jan, S.U.; Hasan, M.N.; Koo, I. A Hybrid LATAM and Few-Shot Learning Framework for Fault Diagnosis in Wireless Sensor Networks. *IEEE Sens. J.* **2025**, *25*, 43102–43116. [CrossRef]

34. Sekar, A.K.; Ramakrishnan, R.; Ganesh, A.; Kiruthiga, T. Emerging cyber security and brute force attacks in hospital management information systems. In Proceedings of the 2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon), Singapore, 18–19 August 2023; pp. 421–426.
35. Verizon Business. How to Prevent Man-in-the-Middle Attacks in Healthcare. Available online: https://www.verizon.com/business/resources/articles/s/how-to-prevent-man-in-the-middle-attacks-in-healthcare/ (accessed on 19 December 2025).
36. ORDR. Rise of the Machines Report 2024. *ORDR* **2024**. Available online: https://ordr.net/resources/rise-of-the-machines-report-2024 (accessed on 16 December 2025).
37. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-middle attack mitigation in Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 2053–2062. [CrossRef]
38. Raoof, M.M.; Aldaghmi, N.; Aljuaid, H. IoT Security in Healthcare: A Recent Trend and Predictive Study of SQL Injection Attacks. *J. Eng.* **2025**, *2025*, e70103. [CrossRef]
39. Peregrin, T. Managing HIPAA compliance includes legal and ethical considerations. *J. Acad. Nutr. Diet.* **2021**, *121*, 327–329. [CrossRef]
40. Chidambaranathan, S.; Geetha, R. Deep learning enabled blockchain based electronic heathcare data attack detection for smart health systems. *Meas. Sens.* **2024**, *31*, 100959. [CrossRef]
41. Ejiofor, O.; Akinsola, A. Securing the future of healthcare: Building a resilient defense system for patient data protection. *arXiv* **2024**, arXiv:2407.16170. [CrossRef]
42. Kavitha, A.; Rao, B.S.; Akthar, N.; Rafi, S.M.; Singh, P.; Das, S.; Manikandan, G. A novel algorithm to secure data in new generation health care system from cyber attacks using iot. *Int. J. Electr. Electron. Res. (IJEER)* **2022**, *10*, 270–275. [CrossRef]
43. Chamoli, A.; Kirsali, A.; Sharma, S. Cyber Attack Prevention Method for Enhanced Privacy of Patients Digital Healthcare Data in Smart Hospitals. In Proceedings of the 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 8–9 August 2024; Volume 1, pp. 54–59.
44. Akinade, S.K. Implementing AI-driven anomaly detection for cyber-security in healthcare networks. *ATBU J. Sci. Technol. Educ.* **2024**, *12*, 598–610.
45. Kilincer, I.F.; Ertam, F.; Sengur, A.; Tan, R.-S.; Acharya, U.R. Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. *Biocybern. Biomed. Eng.* **2023**, *43*, 30–41. [CrossRef]
46. Ünözkan, H.; Ertem, M.; Bendak, S. Using attack graphs to defend healthcare systems from cyberattacks: A longitudinal empirical study. *Netw. Model. Anal. Health Inform. Bioinform.* **2022**, *11*, 52. [CrossRef]
47. ul Sami, I.; Ahmad, M.B.; Asif, M.; Ullah, R. DoS/DDoS detection for E-Healthcare in internet of things. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 297–300.
48. Minocha, S.; Joshi, K.; Sharma, A.; Namasudra, S. Research challenges and future work directions in smart healthcare using IoT and machine learning. *Adv. Comput.* **2025**, *137*, 353–381.
49. Premchand, P.; Lakshmi, M.V.; Zameer, S.R.; Rao, V.S.; Krishna, K.G. The SQL Injection Uses Malicious Code to Manipulate Your Database into Revealing Information. *Fuzzy Syst. Soft Comput.* **2025**, *16*, 244–251.
50. Harper, C. Role-Based Access Control (RBAC) and Encryption Techniques for Enhancing Relational Database Security. *Res. Prepr.* **2025**. Available online: https://www.researchgate.net/publication/392346447_ROLE-BASED_ACCESS_CONTROL_RBAC_AND_ENCRYPTION_TECHNIQUES_FOR_ENHANCING_RELATIONAL_DATABASE_SECURITY (accessed on 12 December 2025).
51. Piskachev, G. Adapting Taint Analyses for Detecting Security Vulnerabilities. Ph.D. Thesis, University of Paderborn, Paderborn, Germany, 2022.
52. Nair, S.S. Securing against advanced cyber threats: A comprehensive guide to phishing, XSS and SQL injection defense. *J. Comput. Sci. Technol. Stud.* **2024**, *6*, 76–93. [CrossRef]
53. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. *Technovation* **2023**, *121*, 102583. [CrossRef]
54. Alabdulatif, A.; Khalil, I.; Saidur Rahman, M. Security of blockchain and AI-empowered smart healthcare: Application-based analysis. *Appl. Sci.* **2022**, *12*, 11039. [CrossRef]
55. Kalapaaking, A.P.; Khalil, I.; Yi, X. Blockchain-based federated learning with SMPC model verification against poisoning attack for healthcare systems. *IEEE Trans. Emerg. Top. Comput.* **2023**, *12*, 269–280. [CrossRef]
56. Alfakeeh, A.S. A blockchain-enabled IoT framework for secure attack detection and advanced feature selection in smart healthcare. *Eng. Technol. Appl. Sci. Res.* **2025**, *15*, 28219–28223. [CrossRef]
57. Alamro, H.; Marzouk, R.; Alruwais, N.; Negm, N.; Aljameel, S.S.; Khalid, M.; Alsaid, M.I. Modeling of blockchain assisted intrusion detection on IoT healthcare system using ant lion optimizer with hybrid deep learning. *IEEE Access* **2023**, *11*, 82199–82207. [CrossRef]
58. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.N.; Shorfuzzaman, M. Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8065–8073. [CrossRef]

59. Javed, M.; Tariq, N.; Ashraf, M.; Khan, F.A.; Asim, M.; Imran, M. Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework. *Sensors* **2023**, *23*, 9372. [CrossRef]
60. Akshay Kumaar, M.; Samiayya, D.; Vincent, P.D.R.; Srinivasan, K.; Chang, C.Y.; Ganesh, H. A hybrid framework for intrusion detection in healthcare systems using deep learning. *Front. Public Health* **2022**, *9*, 824898. [CrossRef] [PubMed]
61. Thilagam, K.; Beno, A.; Lakshmi, M.V.; Wilfred, C.B.; George, S.M.; Karthikeyan, M.; Karunakaran, P. Secure IoT healthcare architecture with deep learning-based access control system. *J. Nanomater.* **2022**, *2022*, 2638613. [CrossRef]
62. Sengan, S.; Khalaf, O.I.; Sharma, D.K.; Hamad, A.A. Secured and privacy-based IDS for healthcare systems on e-medical data using machine learning approach. *Int. J. Reliab. Qual. E-Healthc.* **2022**, *11*, 1–11. [CrossRef]
63. Ali, A.; Ali, H.; Saeed, A.; Ahmed Khan, A.; Tin, T.T.; Assam, M.; Mohamed, H.G. Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning. *Sensors* **2023**, *23*, 7740. [CrossRef]
64. Ali, A.; Pasha, M.F.; Ali, J.; Fang, O.H.; Masud, M.; Jurcut, A.D.; Alzain, M.A. Deep learning based homomorphic secure searchable encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors* **2022**, *22*, 528. [CrossRef] [PubMed]
65. Al-Otaibi, S.; Ayouni, S.; Sarwar, N.; Irshad, A.; Ullah, F. AI-driven security framework for medical sensor networks: Enhancing privacy and trust in smart healthcare systems. *Clust. Comput.* **2025**, *28*, 408. [CrossRef]
66. Rodriguez, W.; Martinez, E.; Hernandez, D.; Lopez, B.; Gonzalez, R.; Wilson, S.; Anderson, J. A Hybrid AI Framework for Detecting Insider Threats in Hospital Information Systems. *ResearchGate* **2025**. Available online: https://www.researchgate.net/profile/Olatunji-Isreal/publication/398453610_A_Hybrid_AI_Framework_for_Detecting_Insider_Threats_in_Hospital_Information_Systems/links/693708f706a9ab54f8450fde/A-Hybrid-AI-Framework-for-Detecting-Insider-Threats-in-Hospital-Information-Systems.pdf (accessed on 16 December 2025).
67. Bonagiri, K.; Nici Marx, V.S.; Gopalsamy, M.; Iyswariya, A.; Reni Hena Helan, R.; Sultanuddin, S.J. AI-driven healthcare cyber-security: Protecting patient data and medical devices. In Proceedings of the 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 28–30 August 2024; pp. 107–112.
68. Sharma, P.; Moparthi, N.R.; Namasudra, S.; Shanmuganathan, V.; Hsu, C.H. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. *Expert Syst.* **2022**, *39*, e12915. [CrossRef]
69. Mhiri, S.; Egio, A.; Compastié, M.; Cosio, P. Proxy re-encryption for enhanced data security in healthcare: A practical implementation. In Proceedings of the 19th International Conference on Availability, Reliability and Security, Vienna, Austria, 30 July–2 August 2024; pp. 1–11.
70. Gupta, K.; Saxena, D.; Rani, P.; Kumar, J.; Makkar, A.; Singh, A.K.; Lee, C.N. An intelligent quantum cyber-security framework for healthcare data management. *IEEE Trans. Autom. Sci. Eng.* **2024**, *22*, 6884–6895. [CrossRef]
71. Mittal, S.; Bansal, A.; Gupta, D.; Juneja, S.; Turabieh, H.; Elarabawy, M.M.; Bitsue, Z.K. Using identity-based cryptography as a foundation for an effective and secure cloud model for e-health. *Comput. Intell. Neurosci.* **2022**, *2022*, 7016554. [CrossRef]
72. Rasheed, A.M.; Kumar, R.M.S. Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT. *Front. Comput. Sci.* **2025**, *7*, 1522184. [CrossRef]
73. Kore, A.; Patil, S. Cross-layered cryptography based secure routing for IoT-enabled smart healthcare system. *Wirel. Netw.* **2022**, *28*, 287–301. [CrossRef]
74. TechMagic. Cyber-Attacks in Healthcare: Types, Risks, and Prevention Strategies. TechMagic Blog. 2024. Available online: https://www.techmagic.co/blog/cyber-attacks-in-healthcare (accessed on 16 December 2025).
75. HIPAA Journal. Healthcare Data Breach Statistics. *HIPAA J.* **2026**. Available online: https://www.hipaajournal.com/healthcare-data-breach-statistics/ (accessed on 8 January 2026).
76. Ogunseye, O. Securing the Future of Healthcare: Addressing Cybersecurity Risks in Legacy Medical IoT Devices. Master's Thesis, Bowie State University, Bowie, MD, USA, 2024.
77. Drake, R.; Ridder, E. Healthcare Cybersecurity Vulnerabilities. In Proceedings of the International Conference on Cybersecurity and Cybercrime, Boston, MA, USA, 16–18 November 2022; Volume 9, pp. 49–56.
78. Ijaz, N.; Banoori, F.; Koo, I. Reshaping bioacoustics event detection: Leveraging few-shot learning (FSL) with transductive inference and data augmentation. *Bioengineering* **2024**, *11*, 685. [CrossRef] [PubMed]
79. Islam, S.; Papastergiou, S.; Kalogeraki, E.-M.; Kioskli, K. Cyberattack path generation and prioritisation for securing healthcare systems. *Appl. Sci.* **2022**, *12*, 4443. [CrossRef]
80. Tanriverdi, H.; Kwon, J.; Im, G. Taming complexity in the cybersecurity of multihospital systems: The role of enterprise-wide data analytics platforms. *MIS Q.* **2025**, *49*, 243–274. [CrossRef]
81. Suleski, T.; Ahmed, M.; Yang, W.; Wang, E. A review of multi-factor authentication in the Internet of Healthcare Things. *Digit. Health* **2023**, *9*, 20552076231177144. [CrossRef]
82. Hasan, M.K.; Ghazal, T.M.; Saeed, R.A.; Pandey, B.; Gohel, H.; Eshmawi, A.A.; Abdel-Khalek, S.; Alkhassawneh, H.M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Commun.* **2022**, *16*, 421–432. [CrossRef]

83. Ul Haq, S.; Singh, Y.; Sharma, A.; Gupta, R.; Gupta, D. A survey on IoT and embedded device firmware security: Architecture, extraction techniques, and vulnerability analysis frameworks. *Discov. Internet Things* **2023**, *3*, 17. [CrossRef]
84. Khan, R.; Saeed, U.; Koo, I. Robust sensor fault detection in wireless sensor networks using a hybrid conditional generative adversarial networks and convolutional autoencoder. *IEEE Sens. J.* **2025**, *25*, 13912–13926. [CrossRef]
85. Nedunoori, V. A Comprehensive Review of Encryption and Protection Techniques for Healthcare Data. *Artif. Intell. Healthc. Inf. Syst.—Secur. Priv. Chall.* **2025**, 147–170.
86. Li, N.; Xu, M.; Li, Q.; Liu, J.; Bao, S.; Li, Y.; Li, J.; Zheng, H. A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. *Secur. Saf.* **2023**, *2*, 2022010. [CrossRef]
87. Khan, R.; Saeed, U.; Koo, I. FedLSTM: A federated learning framework for sensor fault detection in wireless sensor networks. *Electronics* **2024**, *13*, 4907. [CrossRef]
88. Nisar, W. Modernization framework to enhance the security of legacy information systems. *Intell. Autom. Soft Comput.* **2022**, *32*, 543–555. [CrossRef]
89. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
90. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.-V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef]
91. George, A.S.; Sagayarajan, S.; Baskar, D.T.; George, A.S. Hovan. Extending Detection and Response: How MXDR Evolves Cybersecurity. *Partners Univers. Int. Innov. J.* **2024**, *2*, 75–84. [CrossRef]
92. Deb, S.; Lupu, E.; Drakakis, E.M.M.; Bharath, A.A.; Leung, Z.K.; Ma, G.R.; Chattopadhyay, A. Securing the Internet of Medical Things (IoMT): Real-World Attack Taxonomy and Practical Security Measures. *arXiv* **2025**, arXiv:2507.19609.
93. Obrik-Uloho, E.P.; Ejiofor, V.O.; Egonwanne, C.H.; Kolo, F.H.O.; Olasege, R.O. Zero-trust architecture for smart hospitals: A virtual blueprint for cyber-resilient healthcare infrastructure. *Arch. Curr. Res. Int.* **2025**, *25*, 166–185. [CrossRef]
94. Topflight Apps. Zero-Trust Architecture in Healthcare: Why It Matters and How It Works. Topflight Apps Blog. 2024. Available online: https://topflightapps.com/ideas/zero-trust-architecture-healthcare/ (accessed on 17 January 2026).
95. FedTech Magazine. Zero trust stands as a secure foundation for the Internet of Medical Things (IoMT). *FedTech Magazine*, 21 May 2024.
96. Shammar, E.; Cui, X.; Zahary, A.; Alsamhi, S.H.; Al-qaness, M.A.A. Threat to trust: A systematic review on Internet of Medical Things security. *J. Parallel Distrib. Comput.* **2025**, *206*, 105172. [CrossRef]
97. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J.* **2021**, *22*, 177–183. [CrossRef]
98. Mazur, S.L.; Sharma, J.B. Medical oversight and public trust of medicine: Breaches of trust. In *The Complex Role of Patient Trust in Oncology*; Springer: Cham, Switzerland, 2024; pp. 35–55.
99. IBM Security. Cost of a Data Breach Report. IBM Security Report. 2024. Available online: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf (accessed on 27 January 2026).
100. Basil, N.N.; Ambe, S.; Ekhator, C.; Fonkem, E.; Nduma, B.N. Health records database and inherent security concerns: A review of the literature. *Cureus* **2022**, *14*, e30168. [CrossRef]
101. Chitta, S.; Crawly, J.; Reddy, S.G.; Kumar, D. Balancing data sharing and patient privacy in interoperable health systems. *Distrib. Learn. Broad Appl. Sci. Res.* **2019**, *5*, 886–925.
102. Ibarra, J.; Jahankhani, H.; Kendzierskyj, S. Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. In *Blockchain and Clinical Trial: Securing Patient Data*; Springer: Cham, Switzerland, 2019; pp. 115–137. [CrossRef]
103. Taiwo, A.E.; Omolayo, O.; Aduloju, T.D.; Okare, B.P.; Oyasiji, O.; Okesiji, A. Human-centered privacy protection frameworks for cyber governance in financial and health analytics platforms. *Int. J. Multidiscip. Res. Growth Eval.* **2021**, *2*, 659–668. [CrossRef]
104. Martínez, A.L.; Pérez, M.G.; Ruiz-Martínez, A. A comprehensive model for securing sensitive patient data in a clinical scenario. *IEEE Access* **2023**, *11*, 137083–137098. [CrossRef]
105. Liddell, K.; Simon, D.A.; Lucassen, A. Patient data ownership: Who owns your health? *J. Law Biosci.* **2021**, *8*, lsab023. [CrossRef]
106. Perwej, Y.; Akhtar, N.; Kulshrestha, N.; Mishra, P. A methodical analysis of medical internet of things (MIoT) security and privacy in current and future trends. *J. Emerg. Technol. Innov. Res.* **2022**, *9*, d346–d371.
107. Jaime, F.J.; Muñoz, A.; Rodríguez-Gómez, F.; Jerez-Calero, A. Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors* **2023**, *23*, 8944. [CrossRef]
108. Joshua, E.S.N.; Bhattacharyya, D.; Rao, N.T. Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: A complete systematic approach. In *Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems*; Academic Press: Amsterdam, The Netherlands, 2022; pp. 291–310. [CrossRef]

109. Sutradhar, K.; Venkatesh, R.; Venkatesh, P. A Review on Smart Healthcare Employing Quantum Internet of Things. *IEEE Eng. Manag. Rev.* **2025**, *53*, 141–153. [CrossRef]
110. Tao, Y.; Zhou, L.; Xie, L.; Zhang, D.; Lei, X.; Xu, F.; Liu, Z. Shardora: Towards Scaling Blockchain Sharding via Unleashing Parallelism. *Cryptol. ePrint Arch.* **2024**, 2024/1896.
111. Sharma, P.; Namasudra, S.; Chilamkurti, N.; Kim, B.-G.; Gonzalez Crespo, R. Blockchain-based privacy preservation for IoT-enabled healthcare system. *ACM Trans. Sens. Netw.* **2023**, *19*, 1–17. [CrossRef]
112. Li, J.; Meng, Y.; Ma, L.; Du, S.; Zhu, H.; Pei, Q.; Shen, X. A Federated Learning Based Privacy-Preserving Smart Healthcare System. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2021–2031. [CrossRef]
113. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1917–1927. [CrossRef] [PubMed]
114. Padinjappurathu Gopalan, S.; Chowdhary, C.L.; Iwendi, C.; Farid, M.A.; Ramasamy, L.K. An efficient and privacy-preserving scheme for disease prediction in modern healthcare systems. *Sensors* **2022**, *22*, 5574. [CrossRef] [PubMed]
115. Ayub, M.S.; Saadi, M.; Koo, I. Optimization of RIS-Assisted 6G NTN Architectures for High-Mobility UAV Communication Scenarios. *Drones* **2025**, *9*, 486. [CrossRef]