

Foundation University
Journal of Engineering and
Applied Sciences

FUJEAS
Vol. 5, Issue 1, 2024
DOI:10.33897/fujeas.v5i1.889

Research Article

Article Citation:

Memon et al. (2024). "Software Level Security, Privacy Attacks and Challenges in Smart Healthcare Systems". *Foundation University Journal of Engineering and Applied Sciences*
DOI:10.33897/fujeas.v5i1.889



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Copyright

Copyright © 2024 Memon et al.



Published by
Foundation University
Islamabad.

Web: <https://fui.edu.pk/>

Software Level Security, Privacy Attacks and Challenges in Smart Healthcare Systems

Sumaira Memon ^{a,*}, Shahzad Memon ^b, Lachhman Das Dhomeja ^a,
Bisharat Rasool Memon ^c, Nisar Ahmed Memon ^d, Muhammad
Kamran ^e

^aAHS Bukhari Postgraduate Centre of Information and Communication Technology
Faculty of Engineering and Technology, University of Sindh, Jamshoro, Pakistan.

^bDepartment of Electronics Engineering, Faculty of Engineering and Technology
University of Sindh, Jamshoro, Pakistan.

^cDepartment of Information Technology, Faculty of Engineering and Technology
University of Sindh, Jamshoro, Pakistan.

^dDepartment of Telecommunication Engineering, Faculty of Engineering and Technology
University of Sindh, Jamshoro, Pakistan.

^eDepartment of Distance Continuing & Computer Education, Faculty of Education,
University of Sindh, Jamshoro, Pakistan.

* **Corresponding author:** sumaira.memon@scholars.usindh.edu.pk

Abstract:

The widespread adoption of smart healthcare systems and the use of IoT, cloud computing, robotics, and Artificial Intelligence for pandemic data analysis, remote diagnostics, the use of wireless medical devices, and public information services has introduced new cybersecurity risks. The vast amount of personal data, including health information, makes healthcare systems a prime target for cybercriminals who could exploit it for harassment and fraudulent purposes. Additionally, the increased reliance on anytime, anywhere connectivity creates vulnerabilities in wireless medical devices. Recent reports highlight these threats, with examples including privacy breaches, ransomware attacks, and disruptions in communication channels for medical devices. Such security breaches can erode patient trust, cripple healthcare systems, and even endanger lives. This surge in usage and integration of smart devices, often connected through healthcare apps, has also introduced new cybersecurity concerns. To address these challenges, this paper reviews the recent software-level security and privacy threats in smart healthcare systems, explores mitigation techniques proposed in the literature, and discusses the vulnerabilities of medical devices along with the service disruption in the communication channel, and the impact of cybersecurity attacks on smart healthcare systems, and discusses the future challenges of software security in smart healthcare.

Keywords: Smart Healthcare; Internet of Things; Cyber Security; Data Privacy;
Software Security.

1. Introduction

Recently, many smart healthcare systems have been proposed, developed, and implemented in various hospitals around the globe [1]. The vision of smart healthcare has been introduced when IoT is used in supporting core functions of healthcare services, including smart beds, patients' smart tables, online access to your health record, and self-service registration. Smart healthcare is highly efficient with various features that

aim to maintain the interoperability of assets, to facilitate traditional hospital infrastructure, to ensure a security and privacy layer on sensitive information, and usability of end-users, to add efficiency to existing hospital processes [2]. Smart environments strictly depend on automated processes and interconnected assets such as wearable devices, smart monitoring instruments, smart phones, computers, and medical devices that smartly provide information, connect people and institutions related to healthcare, and actively manage and respond to the smart healthcare environment in an intelligent manner. However, IoT-based medical devices are not protected from cybercriminals and have proven to be a big threat to smart hospitals, such as patient monitoring, leakage of patient personal information, and delays in the monitoring response of smart healthcare. Third-party failures, human errors, and system breakdowns are considered threats to smart hospitals. These concerning risks and vulnerabilities are handled by a mix of organizational and technological measures. The two factors (organization and technology) are also combined to introduce new possibilities for inpatient care, like remote medical treatment, enhanced patient security, smooth patient flow, increased diagnostics/surgical capability, trustworthiness, and cyber-resilience [2]. However, the growing reliance on ICT also brings new problems with it.

Securing patient data must be a top priority in healthcare. Healthcare systems store a wide range of sensitive information, such as medication details, medical histories, and patient discharge records. Nowadays, healthcare systems are mostly computerized, with data stored electronically, which improves healthcare operations and facilitates information exchange [1]. As smart healthcare systems are increasingly being implemented in hospitals worldwide, new security challenges have emerged. One of them is data security and privacy. While these systems offer numerous benefits, they must be equipped with robust security and privacy measures to protect patient data effectively.

Several smart healthcare software, like remote care systems, identification systems, networking technology, and integrated clinical information systems, are available to explore. Among these clinical information systems are software that can be used in the diagnostic laboratory, clinic, pharmacy, and blood bank of the hospital. Interconnected clinical systems, along with medical equipment and identification components, are used in smart hospitals to allow smart end-to-end patient care procedures that are highly capable of making autonomous choices. Hence, all these require utmost security and privacy. This review provides a comprehensive analysis of software security in healthcare systems, focusing on the most common attacks identified in the literature. It aims to enhance the understanding of mitigation techniques that can be employed to protect healthcare systems from data breaches and cyberattacks. Additionally, this paper discusses the various types of security attacks, vulnerabilities, challenges, and the mitigation strategies proposed in existing research.

2. Related Work

The healthcare sector is frequently highlighted for cybersecurity attacks, as suggested by reports indicating an increase in the number of attacks, including medical identity theft and breaches of millions of records [2], [3]. Lyn Coventry and Dawn Branley [4] conducted research by searching the PubMed database for peer-reviewed articles from April 2012 to April 2018 using keywords such as "cyber security" and "healthcare". This search initially retrieved 2,475 articles, which were further narrowed down to 1,249 articles from 2014 to 2018. These articles highlight issues such as hacking, phishing, and data breaches in healthcare settings. Software security and privacy attacks are events that can grant unauthorized access to attackers, potentially leading to data breaches and causing damage to software and its users. These malicious activities impact software security and privacy in various ways. The healthcare sector has adopted new technologies but still relies on older versions of software, making it more vulnerable to exploitation. Attacks such as hacking and malware can often go undetected. Moreover, IT teams are unable to access the internal software of medical devices, relying entirely on manufacturers to maintain device security.

Hematology, chemistry, immunology, and blood banking are just a few areas of laboratory science that rely on laboratory information system (LIS) software. While LIS plays a vital role in various healthcare

settings, its complexity can present challenges. When errors occur, significant effort is required to get the system back up and running. Additionally, system growth necessitates ongoing updates and employee training. Furthermore, current reporting systems often have limited data source options [5]. Most LIS systems are software-based and struggle to integrate data from other crucial healthcare systems like pathology, payroll, and billing.

Despite the challenges of LIS, technology is revolutionizing healthcare delivery. Doctors now have access to a range of user-friendly devices like digital ECGs (electrocardiograms), ventilators, and wireless temperature monitors. Studies like the one conducted in Manhattan [5] show a high smartphone usage among healthcare users, opening doors for mobile health applications.

These advancements allow doctors to remotely examine and diagnose patients, collect data more efficiently, and potentially create a centralized system that connects various hospital devices. Such a system would enable remote monitoring of operations and various lab tests. Laboratories can be further optimized by allowing online test requests from doctors and online delivery of results. Touch-based interfaces and smartphones can also improve time management and access to reports. However, the increasing reliance on technology necessitates robust cybersecurity measures. Data breaches in healthcare have been on the rise, with healthcare data being a prime target for cybercriminals due to sensitive personal and healthcare information. Data breaches in the healthcare sector have been rising since 2010, according to a report by HIPPA journal [6].

A lack of resource allocation for security in the healthcare sector, combined with insufficient funding, can create system vulnerabilities that ultimately contribute to cyberattacks [7], [8]. The healthcare sector is often targeted by cybercriminals, hacktivists, and political interests for financial or political gain, or to expose its vulnerabilities. A summary of published literature on cybersecurity attacks is illustrated in Table 1.

Table 1: Literature review related to cybersecurity attacks on smart healthcare systems

Year	Author Name	Title of Article	Review and Limitations of Research
2023	Elham Abdullah Al-Qarni.	Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies [9]	A cybersecurity attack can have a significant impact on a patient's reputation, compromise patient data, and lead to financial losses. Due to this, healthcare institutions have a dire need for robust cybersecurity measures. This article focuses on the steps required to protect patient data and mitigate the effects of system errors and other related issues.
2022	Ismail Keshta.	AI-driven IoT for smart healthcare: Security and privacy issues [10]	In Smart healthcare system threats such as data eavesdropping, confidentiality breaches, and Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) attacks target Internet-of-things (IoT) components. and making privacy a major concern for healthcare systems This study suggests that AI-driven IoT requires an advanced and well-defined architecture to enhance user privacy and security.
2021	Khadija Abu Ali, Sarah Al Younis.	Cyber Security in the Healthcare Industry [11]	This paper reviews the existing literature, highlighting that while healthcare has advanced, it has also become more vulnerable to cyberattacks due to primitive defense mechanisms. The risk of attacks has increased due to the presence of valuable data. No novel approach has been discussed.

2021	Nicole M. Thomasian, Eli Y. Adashi.	Cybersecurity in the Internet of Medical Things [12]	The advancement in healthcare systems has made patient data more vulnerable, requiring continuous monitoring by cybersecurity personnel to detect new attack methods and vulnerabilities. This paper discusses novel threats and cybersecurity regulations related to the Internet of Medical Things (IoMT).
2020	D. N. Mohan, S. Sagar Gowda, I. S. Vikyath.	Cyber Security in Healthcare [13]	Healthcare data is an easy target due to weak defense mechanisms. Common cybersecurity breaches include health information theft, ransomware attacks on hospitals, and threats to human life. This paper discusses these prevalent security threats and data security issues.
2020	S. T. Argaw et al.	Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks [14]	When healthcare data is compromised, it poses a risk to the psychological well-being of patients. It has also been noted that data breaches have increased since 2010. This research suggests that a risk-based approach is urgently needed, starting with the identification of risks and followed by proper risk management. Furthermore, no proper risk assessment model has been consistently followed.
2020	Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, et al.	Healthcare Data Breaches: Insights and Implications [15]	Between 2005 and 2019, 64% of Electronic Health Records (EHRs) were compromised, with hacking being the primary attack method. This study suggests that preventive measures should be a top priority for researchers, security experts, and healthcare organizations. Relevant aspects should be thoroughly examined, and further research is warranted in several areas.
2020	Mohammad Zarour, Mamdouh Alenezi, Md Tarique Jamal Ansari, et al.	Ensuring data integrity of healthcare information in the era of digital health [16]	This paper addresses the digital health issue of data breaches, referencing a HIPAA study that identifies the 25 largest data breaches in the healthcare industry. It demonstrates that hacking is the most common cause of medical data breaches.
2019	Shariq Aziz and Arshad Ali.	IoT Smart Health Security Threats [17]	This study discusses cyberattacks such as Denial of Service (DoS), snooping, routing attacks, sensor attacks, and replay attacks on smart health monitoring systems. It highlights how these attacks can manipulate patient data and disrupt medical services. The study also proposes potential solutions to mitigate these cyber threats.
2024	Abbasi, Nasrullah, and Derek A. Smith.	Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA compliance framework, and the responsibilities of healthcare providers [18]	This study discusses cybersecurity issues like hacking, phishing, and data breaches, specifically in the healthcare setting, organizational practices, and health technology development. Also, emphasize the need for awareness and actions at multiple levels.

In 2023, the healthcare industry experienced a distressing milestone, as it reported 725 significant security breaches to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). This surpassed the previous year's record of 720 breaches. Unfortunately, this trend of increasing security breaches has been ongoing, with only a brief respite in 2015. However, there is a glimmer of hope, as the rate of increase seems to be slowing down. It is possible that in 2024, the healthcare industry may finally begin to reverse this troubling trend.

3. Common Software Security Threats

3.1. Malware and Phishing Attempts

Malware and phishing attacks pose a significant threat to healthcare systems. Often installed through malicious scripts or stolen login credentials, they can compromise the entire network. A key challenge with malware is that a seemingly harmless connection can introduce malicious activity. These scams often involve emails requesting information, granting hackers access upon submission. One frequent scam involves receiving emails from websites requesting information. If people submit this information, hackers can access it and get into the system. One of the cases has been reported in Hancock Regional Hospital (United States). It is a small hospital with 71 beds in Greenfield, Indiana, founded in 1951. On 11 January 2018, a malware named SamSam [19] attacked this hospital and targeted their emergency IT backup system server and circulated via electronic connections between the backup site, located miles from the main campus, and the server farm at the hospital [20]. Later, it was discovered that backup files from many systems had been permanently corrupted, apart from electronic medical record backup files. The attack was conducted with the help of Microsoft's Remote Desktop Protocol (RDP). Educating employees to recognize phishing attempts is crucial.

3.2. Vendors

Due to a lack of upfront security considerations by many vendors selling products to the healthcare industry [21], securing all access points to computer systems becomes a challenge. While regular system maintenance is crucial, it can introduce vulnerabilities if the hardware vendor's administrative account remains accessible and unguarded. Hackers can exploit this very access to launch attacks.

3.3. Unsecured Mobile Devices

Mobile logins in healthcare facilities present a significant security challenge. Unlike traditional login methods, they often lack inherent security features on the user device itself. This makes it vulnerable, which is easily exploitable by many hackers. Sensitive information such as passwords and network credentials can be exposed, potentially granting unauthorized access to healthcare systems. To mitigate these risks, healthcare organizations must implement robust security protocols. These may include strong password requirements, multi-factor authentication, and device management policies. A complete ban on user devices, however, might be overly restrictive and hinder workflow.

3.4. Unrestricted Access to Computers

Unrestricted computers pose a significant security risk in healthcare settings where they are connected to a network containing sensitive patient information. These readily accessible devices can be exploited by unauthorized personnel or hackers. Phishing attempts on these computers can act as a gateway, granting access to the more secure areas of the network. This involves implementing access controls to restrict who can use specific computers and ensuring patient information is stored in secure, designated locations.

4. Data Breaches and Cyber Attacks in Smart Healthcare Systems

For modeling software security and privacy attacks in healthcare systems, various software tools and hardware platforms are used for experimentation. The choice of tools and platforms often depends on the specific needs of the research. Hardware platforms such as IoT devices, network equipment, computers, and servers can be employed for testing purposes. IoT devices like smart medical sensors, health monitors, and smart infusion pumps can be used to simulate real-world healthcare environments. Computers can be utilized for performing simulations, conducting security tests, and mimicking the healthcare IT infrastructure.

Numerous software tools are available to assist in experimentation. These include security testing tools, simulators and emulators, network analyzers, and custom security frameworks. Some examples include:

- **Security Testing Tools:** Tools like Burp Suite and Nessus can be used to scan for vulnerabilities, perform penetration testing, and identify weaknesses in software systems.
- **Network Analyzers:** Wireshark can help analyze network traffic, track activities, and detect potential data breaches.
- **Simulators and Emulators:** Tools like GNS3 and Packet Tracer provide simulated environments for network experiments.
- **Custom Security Frameworks:** These frameworks are often designed by researchers or adapted from existing standards to meet the specific needs of healthcare software testing [22].

Despite the growing adoption of electronic health records (EHRs), cybersecurity considerations often lag. Behind this critical gap lies healthcare systems vulnerable to devastating cyberattacks. A 2017 report [23] documented the sale of Australians' health records on the dark web [24]. Ransom attacks have also crippled hospitals in the UK's NHS and the US [25]. These incidents (see Figure 1) demonstrated the potential for cyberattacks to paralyze entire healthcare systems [26].

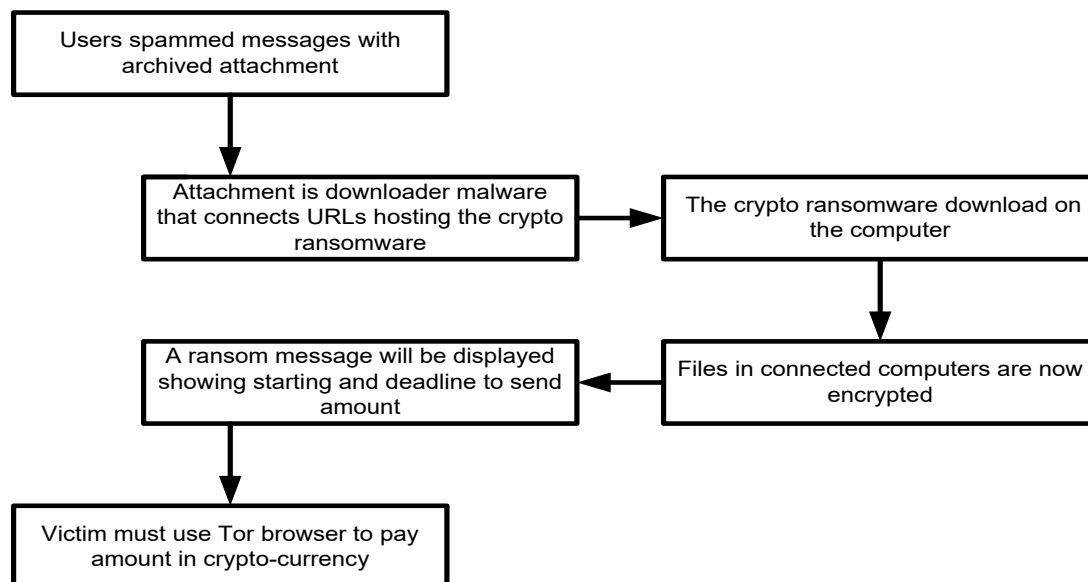


Figure 1: Ransomware attack scenario

The evolving healthcare industry increasingly relies on interconnected devices, creating a vast network with a growing number of potential cyber vulnerabilities. These record-breaking levels of connectivity introduce multiple entry points for attackers, as shown in Figure 2, making data like that shown in Figure 1 more likely to go unnoticed. Even before the digital age, privacy breaches were a concern, and a single data leak can impact millions [27]. A recent survey highlights that a significant portion of healthcare breaches occur within business associates [26]. In conclusion, the rise of interconnected

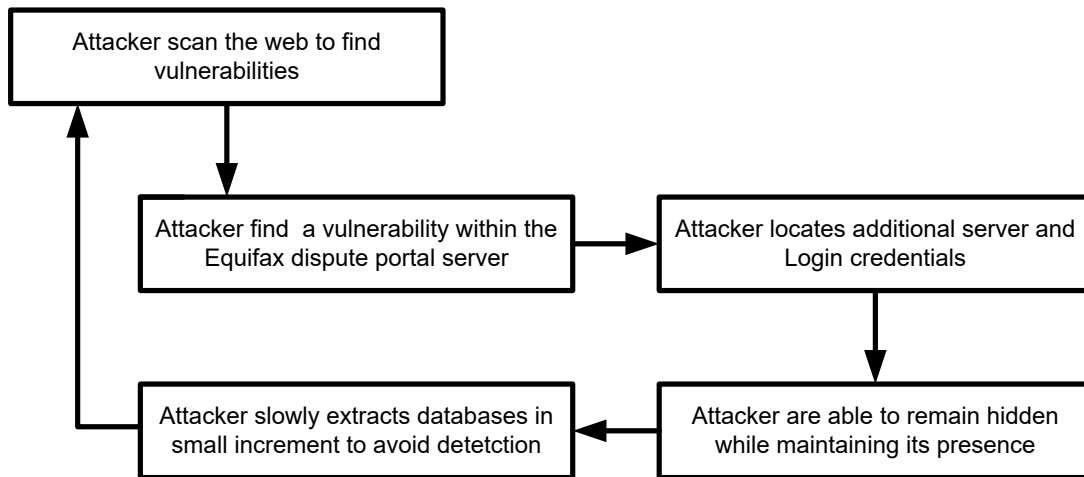


Figure 2: Theft of data

devices necessitate increased investment in cybersecurity measures to safeguard healthcare equipment and patient data.

A staggering number of data breaches plagued various industries between 2005 and 2019, with over 10 billion records compromised across sectors like healthcare (MED), business services (BSF &BSO), education (EDU), and government (GOV) [28], [15]. The healthcare industry stands out as the most affected, suffering & staggering 3,912 documented breaches and accounting for a concerning 43.38% of all compromised data during this period. Hacking (HACK) was the primary culprit behind these breaches, compromising over 64% of healthcare data in 2019. This reliance on hacking has grown even more worrisome in recent years, with hacking attacks responsible for over 92% of exposed data between 2015 and 2019. While hacking dominated, other breach types like physical access (PHYS) and lost or stolen devices (PORT) also played a role, contributing 14.39 % and 9.51% of compromised healthcare data, respectively [28], [15].

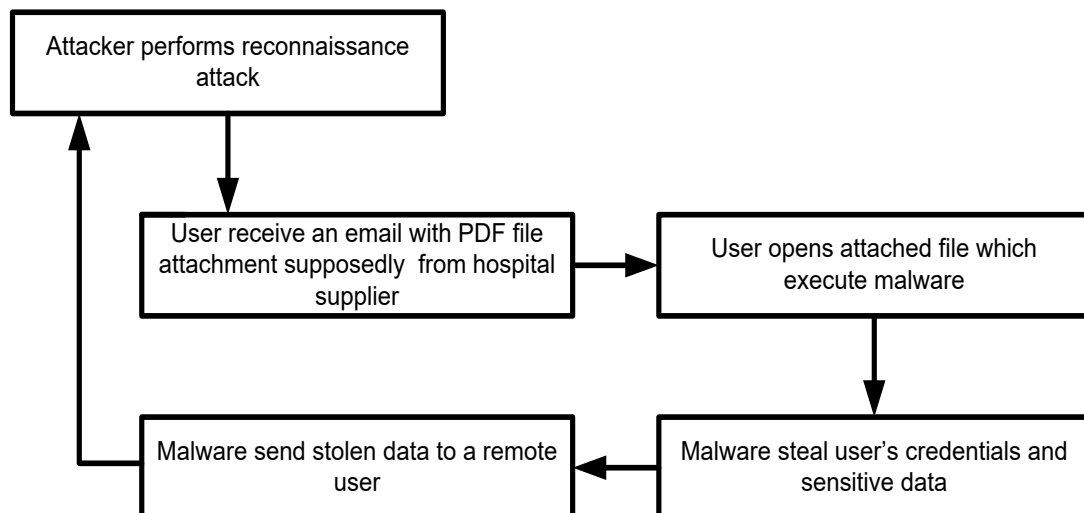


Figure 3: Hacking of a healthcare system

A study analyzing the 25 largest healthcare data breaches over the past decade reveals hacking (see Figure 3) as the most prevalent attack method according to HIPAA data [6]. This finding is particularly concerning because healthcare organizations may be underestimating the true prevalence of hacking incidents. The low reported percentage of hacking attempts might be due to a lack of detection in previous years, suggesting that historical data may not fully capture the current threat landscape.

Table 2 summarizes the recent cyberattacks on healthcare data, potentially including data integrity issues.

Table 2: Summary of recent attacks on software security in healthcare systems

Year	Name of Attack	Impact of an attack on System Security and Privacy
2024	Ransomware [29], [30]	Ransomware attacks have targeted healthcare providers and had a severe impact on patient care and data security.
2023	Ransomware/Phishing [31], [32]	According to the report, ransomware attacks mostly begin by using phishing and exploiting vulnerabilities. Reports indicate a 94% increase in ransomware attacks on healthcare organizations from 2021 to 2022.
2022	Ransomware/Data breach [33]	Ransomware remained a predominant threat in 2022, with over 51 million records compromised across 701 data breaches, marking a 13.1% increase in breached records compared to previous years.
2021	Ransomware [6]	In 2021, ransomware attacks increased by 94% compared to the previous year.
2020	Ransomware [34], [35]	Recently, in October 2020, Eddy and Perlotha reported on a ransomware cyber-attack that resulted in a patient's death.
2019	Hacking [26]	Exposing the data of 25 million patients. Health data was compromised.
2018	Malware [27], [36]	Malware targeted the three-tiered IT backup system server of Hancock Regional Hospital. The malware was likely released through an electronic connection between the backup sites at the main campus and the server located at the hospital itself.
2017	Ransomware Wanna-Cry [24], [37]	The Wanna-Cry ransomware attack, which infected over 300,000 computers, demanded ransom payments in Bitcoin. It brings the US hospitals' health care system to a standstill.
2017	Ransomware [38], [39]	Unique health records of Australians have been kept for sale on the dark web.
2016	Social Engineering [40], [41]	The hospital immediately shut down all its servers and computers to protect the overall systems.

The rapid adoption of electronic health records (EHRs) has revolutionized healthcare delivery and improved clinical outcomes. However, this progress has been accompanied by a growing concern about data security. Healthcare data is a goldmine for cybercriminals due to its sensitive nature and the potential for financial gain. Breaches involving stolen health information (see Table 2), ransomware attacks crippling hospitals, and even assaults on implanted devices can all erode patient trust and endanger lives. This is why cybersecurity is paramount to patient safety. Fortunately, new regulations and policies are emerging to drive positive change. However, a truly inclusive solution requires a multi-pronged approach that involves technological advancements, updated procedures and practices, and changes in human behavior.

5. Mitigating Data Security Challenges

After COVID-19, the need to adopt smart healthcare became essential in the healthcare sector, and it faces challenges of cybersecurity, which impact patient data security and privacy. To ensure patient

data security, it is crucial to develop and promote a culture of cybersecurity awareness for healthcare staff alongside implementing standard data security procedures [42]. Interactive training on understanding cybersecurity and privacy, and regular communication, is crucial for healthcare staff working at all levels. These sessions empower healthcare staff to understand, identify, and mitigate cyber threats impacting patient data and privacy. Moreover, standard security protocols need to be implemented for both physical and virtual technological assets of healthcare. To assess their effectiveness, these protocols should be regularly audited and tested. Several measures are required to strengthen these protocols, including:

- Implementing access control to restrict unauthorized access.
- Use of intrusion detection and prevention systems to monitor healthcare network traffic.
- Transmitting data using VPNs and up-to-date healthcare software.
- Device firmware and conducting regular penetration testing to proactively identify and address security vulnerabilities of healthcare services and systems.

While managing these processes can be complex, partnering with a specialized external security agency can offer comprehensive solutions and ongoing support. This frees healthcare employees to focus on their core competence. Whereas cyber-attacks, which can be mitigated by these measures, are discussed in Table 3 below.

Table 3: Cyber-attacks and their mitigation measures

Cyber-Attack	Mitigation Measure
Phishing Attack, Social Engineering, and Brute Force	Implementing access control to restrict unauthorized access,
Network Intrusion and DDoS, Hacking, Ransomware	Use of intrusion detection and prevention systems to monitor healthcare network traffic
Man-in-the-Middle Attack and Eavesdropping	Transmitting of data using VPNs, up-to-date healthcare software
Hacking Ransomware	Device firmware and conducting regular penetration testing to proactively identify and address security vulnerabilities of healthcare services and systems.

6. Conclusion

The healthcare dependence on electronic healthcare records has increased with the emergence of new technologies. Moreover, healthcare systems' round-the-clock connectivity made it a prime target for cybercriminals. Regulations like HIPPA have become more widespread, and as healthcare data has moved online, vulnerabilities in healthcare systems have grown. A 2011 Redspin report highlights this concern, revealing that nearly 19 million patients were affected by breaches that year, with business associates responsible for a significant portion (59%). These breaches were not only caused by malicious actors but also by accidental losses or theft of devices such as laptops, which pose a serious threat. Cybersecurity vulnerabilities of healthcare systems have been extending beyond stolen patient data. Breaches of networked laboratory equipment and facility controls can be sensitive due to scientific and business data, intellectual property, and even physical security. Cyber-attacks can have severe consequences, including financial losses, reputational damage, and disruptions to critical services. Denial-of-service attacks, virus outbreaks, and unauthorized access to sensitive information can jeopardize a healthcare organization's sustainability. This review emphasizes the critical need for robust cybersecurity measures in healthcare and discusses its mitigating challenges.

Many breaches occur due to inadequate security procedures and a lack of awareness of vulnerabilities within organizations. Healthcare data is highly susceptible to attack, and healthcare organizations must prioritize data security to protect patients, finances, and reputations.

7. References

- [1] E. Li, J. Clarke, A. L. Neves, H. Ashrafiyan, and A. Darzi, "Electronic Health Records, Interoperability and Patient Safety in Health Systems of High-income Countries: A Systematic Review Protocol," *BMJ Open*, vol. 11, no. 7, Jul. 2021, doi: 10.1136/BMJOPEN-2020-044941.
- [2] A. H. Seh *et al.*, "Healthcare Data Breaches: Insights and Implications," *Healthc. (Basel, Switzerland)*, vol. 8, no. 2, Jun. 2020, doi: 10.3390/HEALTHCARE8020133.
- [3] "66% of Healthcare Organizations Say Patient Care was Disrupted by a Cyberattack." [Online] <https://www.hipaajournal.com/66pc-healthcare-organizations-patient-care-disruption-cyberattack/> [Accessed Sep. 10, 2024].
- [4] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/J.MATURITAS.2018.04.008.
- [5] V. Thakare and G. Khire, "Role of Emerging Technology for Building Smart Hospital Information System," *Procedia Econ. Financ.*, vol. 11, pp. 583–588, 2014, doi: 10.1016/s2212-5671(14)00223-8.
- [6] S. Alder, "Security Breaches in Healthcare in 2023," 2024. [Online]. Available: <https://www.hipaajournal.com/security-breaches-in-healthcare/>.
- [7] R. Abdolkhani, K. Gray, A. Borda, and R. DeSouza, "Recommendations for the Quality Management of Patient-Generated Health Data in Remote Patient Monitoring: Mixed Methods Study," *JMIR mHealth uHealth*, vol. 11, 2023, doi: 10.2196/35917.
- [8] "An Executive View of Key Cybersecurity Trends and Challenges in 2023,". [Online] <https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023> [Accessed Sep. 10, 2024].
- [9] E. A. Al-Qarni, "Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, pp. 135–140, 2023, doi: 10.14569/IJACSA.2023.0140513.
- [10] I. Keshta, "AI-driven IoT for smart health care: Security and privacy issues," *Informatics Med. Unlocked*, vol. 30, p. 100903, Jan. 2022, doi: 10.1016/J.IMU.2022.100903.
- [11] K. A. Ali and S. Alyounis, "CyberSecurity in Healthcare Industry," *2021 Int. Conf. Inf. Technol. ICIT 2021 - Proc.*, pp. 695–701, Jul. 2021, doi: 10.1109/ICIT52682.2021.9491669.
- [12] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Health Policy and Technology*, vol. 10, no. 3. Elsevier, p. 100549, Sep. 01, 2021, doi: 10.1016/j.hlpt.2021.100549.
- [13] G. V. Mohan, "Cyber Security in Healthcare - IJRESM_V3_I1_145," *Int. J. Res. Eng. Sci. Manag.*, vol. 3, no. 1, pp. 3–5, 2020.
- [14] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, Jul. 2020, doi: 10.1186/S12911-020-01161-7.
- [15] A. H. Seh *et al.*, "Healthcare data breaches: Insights and implications," *Healthcare (Switzerland)*, vol. 8, no. 2. MDPI AG, Jun. 01, 2020, doi: 10.3390/healthcare8020133.
- [16] M. Zarour *et al.*, "Ensuring data integrity of healthcare information in the era of digital health," *Healthc. Technol. Lett.*, vol. 8, no. 3, pp. 66–77, 2021, doi: 10.1049/htl2.12008.
- [17] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT Smart Health Security Threats," *Proc. - 2019 19th Int. Conf. Comput. Sci. Its Appl. ICCSA 2019*, no. August, pp. 26–31, 2019, doi: 10.1109/ICCSA.2019.000-8.
- [18] N. Abbasi, and D. A. Smith, "Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPAA compliance framework and the responsibilities of healthcare providers," *Journal of Knowledge Learning and Science Technology*, vol. 3, no. 3, pp. 278-287, 2024. doi: 10.60087/jkfst.vol3.n3.p.278-287
- [19] "SamSam Ransomware Campaigns | Secureworks." [Online] <https://www.secureworks.com/research/samsam->

- ransomware-campaigns [Accessed Sep. 26, 2022].
- [20] "The Cyber Attack - From the POV of the CEO - Hancock Regional Hospital." [Online] <https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/> [Accessed Sep. 26, 2022].
- [21] B. Kelly, C Quinn, A. Lawlor, R. Killeen, and J. Burrell, "Cybersecurity in healthcare," In *Trends of artificial intelligence and big data for e-health*, pp. 213-231. Cham: Springer International Publishing, 2023.
- [22] "The Ultimate List of 22 Penetration Testing Tools [2024] - The CTO Club." [Online] <https://thectoclub.com/tools/best-penetration-testing-tools/> [Accessed Sep. 10, 2024].
- [23] "Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats." [Online] <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=7dc6aa486b61> [Accessed Sep. 26, 2022].
- [24] "The Medicare machine: patient details of 'any Australian' for sale on darknet | Medicare Australia | The Guardian." [Online] <https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet> [Accessed Sep. 26, 2022].
- [25] S. Mansfield-Devine, "Ransomware: taking businesses hostage," *Netw. Secur.*, vol. 2016, no. 10, pp. 8–17, Oct. 2016, doi: 10.1016/S1353-4858(16)30096-4.
- [26] J. C. Looi, R. C. Looi, P. A. Maguire, S. Kisely, T. Bastiampillai, and S. Allison, "Psychiatric electronic health records in the era of data breaches—What are the ramifications for patients, psychiatrists and healthcare systems?," *Australasian Psychiatry*, vol. 32, no. 2, pp. 121-124, 2024. doi: <https://doi.org/10.1177/10398562241230816>
- [27] "Healthcare data breaches reach record high in April | Modern Healthcare." [Online] <https://www.modernhealthcare.com/cybersecurity/healthcare-data-breaches-reach-record-high-april> [Accessed Sep. 26, 2022].
- [28] M. Zarour *et al.*, "Ensuring data integrity of healthcare information in the era of digital health," *Healthc. Technol. Lett.*, vol. 8, no. 3, pp. 66–77, Jun. 2021, doi: 10.1049/htl2.12008.
- [29] "Cyberattack forces major US health care network to divert ambulances from hospitals | CNN Business." [Online] <https://edition.cnn.com/2024/05/10/tech/cyberattack-ascension-ambulances-hospitals/index.html> [Accessed May 20, 2024].
- [30] "Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic | Acta Criminologica : African Journal of Criminology & Victimology." [Online] https://journals.co.za/doi/abs/10.10520/ejc-crim_v34_n3_a10 [Accessed Nov. 30, 2024].
- [31] "Q2 2022 Threat Landscape: Ransomware Returns, Healthcare Hit." [Online] <https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2022-threat-landscape-ransomware-healthcare-hit> [Accessed May 20, 2024].
- [32] K. Perova, "Creating guidelines and best practices against phishing and ransomware attacks for healthcare personnel," 2022. [Online]. Available: <https://lutpub.lut.fi/handle/10024/164184> [Accessed Nov. 30, 2024]
- [33] "Ransomware Trends, Statistics and Facts Heading Into 2024." [Online] <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts> [Accessed May 20, 2024].
- [34] "Cyber Attack Suspected in German Woman's Death - The New York Times." [Online] <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomware-death.html> [Accessed Sep. 26, 2022].
- [35] S. Schmeelk, "Risk in Healthcare Information Technology: Creating a Standardized Risk Assessment Framework," *Comput. Commun.*, Jan. 2022, doi: 10.5772/INTECHOPEN.96456.
- [36] "Understanding Controls to Detect and Mitigate Malicious Privileged User Abuse - ProQuest." [Online] <https://www.proquest.com/openview/3879636d67ac0a70ec51fcddeb5b340a/1?pq-origsite=gscholar&cbl=44156> [Accessed Nov. 30, 2024].
- [37] S. Krishnan, "Cyber security in healthcare : A narrative review of trends, threats and ways forward," pp. 11–17, 2020.
- [38] "Ponemon Study Shows the Cost of a Data Breach Continues to Increase | Ponemon Institute." [Online] <https://www.ponemon.org/news-updates/news-press-releases/news/ponemon-study-shows-the-cost-of-a-data-breach-continues-to-increase.html> [Accessed Sep. 26, 2022].
- [39] D. R. Hayes, F. Cappa, and J. Cardon, "A Framework for More Effective Dark Web Marketplace Investigations," *Inf. 2018*,

Vol. 9, Page 186, vol. 9, no. 8, p. 186, Jul. 2018, doi: 10.3390/INFO9080186.

- [40] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1. BioMed Central Ltd, Jul. 03, 2020, doi: 10.1186/s12911-020-01161-7.
- [41] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, pp. 1–10, Jul. 2020, doi: 10.1186/S12911-020-01161-7/PEER-REVIEW.
- [42] "The Importance of Cybersecurity Awareness Training for Employees | Institute of Data." [Online] <https://www.institutedata.com/us/blog/cybersecurity-awareness-training/> [accessed May 21, 2024].