GKU Journal of Multidisciplinary Research (GKUJMR)

A Comprehensive Review of Cyber-Attacks in Healthcare

[1] Mr. Sukhdeep Singh, [2] Dr. Shalu Gupta, [3] Mrs. Sukhwinder Kaur

[1]Student, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India
[2]Associate Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India
[3]Assistant Professor, Department of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India

Email ID: [1] sukhdeepsinghgill978@gmail.com, [2] shalu2324@gku.ac.in, [3] reetaman2013@gmail.com

Accepted: 26.11.2025 Published: 26.12.2025 DOI: 10.5281/zenodo.18410022

Abstract – Healthcare systems are key components of national critical infrastructure thinking to support both medical services and the medical responder side of things, as well as long-term patient care. While clinical workflows were modernized with the adoption of digital technologies—including electronic health records (EHRs), telemedicine, Internet-connected medical devices, and cloud-based platforms—they have also expanded the attack surface for cybercriminals. Cyber-attacks on healthcare organizations have tripled over the past ten years, with it now being one of the most attacked sectors internationally. Such incidents can expose private information about patients, interrupt routine medical services, endanger patients, and prevent a country from responding properly in public health crises.

This narrative review provides an overview of developments in healthcare cyber-attacks over the past decade (2009–2019); their adverse effects on patients, providers, and hospital infrastructure; and the techniques that attackers typically employ. The report also highlights some of the responses made by hospitals during prolonged outages of their systems and provides recommendations to improve hospital preparedness for such cyberattacks.

Keywords: Cyber-attacks, ransomware, healthcare cybersecurity, EMR downtime, preparedness, medical device security

I. INTRODUCTION

Object detection and recognition form an essential component of image processing and have emerged as a significant research area within the domains of image processing and pattern recognition [17, 18]. With the global healthcare environment constantly changing with advancements such as EMRs, artificial intelligence, cloud services, and telehealth platforms, modernity and efficiency have come from improved accuracy, accessibility, and coordination of care with medical information systems. But all these benefits are shadowed by the increased cyber security threats towards healthcare institutes due to the increased digital dependency. An attack on the healthcare system is any malicious operation to gain unauthorized access to or disrupt clinical operations or change health information systems (e.g., EMRs, medical devices, imaging systems, hospital networks). Edge detection is commonly used in many research fields such as computer vision, machine learning and pattern recognition [19, 20].

Healthcare organizations are uniquely susceptible to cyber-attacks, as any compromise poses a direct risk to patient lives. Attacks could halt lab reporting, disable medication administration systems, disrupt surgical services, and server-sustaining devices include, ventilators, insulin pumps, or pacemakers. Wasserman & Wasserman [1]. Then, there are laws such as HIPAA that demand hospitals safeguard patient data, and this makes hospitals liable to significant financial and legal repercussions in the aftermath of a breach.

Outdated medical devices contribute to cybersecurity challenges, and a lack of standardized, comprehensive, rigorously tested security protocols as well as vulnerabilities in telehealth applications247. According to a recent report, the number of healthcare data breaches has increased 3X in the last 10 years (Alder, 2024) [2]. The records of patients are regularly sold in the black market for more than $1,000 per copy (IBM, 2024) [11] and this makes hospitals a regular target for cybercriminals.

According to a report from Kroll for 2024, 26% of healthcare prove very low cyber maturity and only 3% even have high-quality threat-monitoring methods (Kroll, 2024) [3]. The takeaway is that these results highlight the importance of proper cyber security and downtime procedures to ensure operational continuity through cyber events.

The aims of this narrative review are as follows:

- Mapping of Cyber Attacks on healthcare organizations since 2009 and Categorizing Attack Trends
- Delve into hospital experiences and operational challenges after losing access to EMR support.
- Provide tangible tips on how to improve cybersecurity readiness and response.

II. METHODS

This narrative review integrates literature regarding cyber-attacks on health care organizations. Google Scholar was chosen as the main database because it indexes a high proportion of open-access publications and retrieves large amounts of full-text scholarly articles. A few years back a Google search for hospital cyberattack returned about 20400 results.

When limiting the search to articles dating between 2020 – 2024 to address recent trends after the COVID-19 pandemic, using the conjunction “hospital” or “cyberattack”, a total of 4,800 results were retained. PubMed served as a secondary database; however, it

generated only 20 viable results, owing to its more specific focus on biomedicine literature.

2.1 Inclusion Criteria

- Articles published in 2020-2024 (2016 on post if particularly relevant)
- English language
- Review articles, original studies, case study, systematic review
- Free full-text availability
- Articles focusing on threat related to healthcare cyber-attacks, EMR Failure, Cyber preparedness or System recovery

2.2 Exclusion Criteria

- Stories that focus just on one part of a hospital
- Articles targeting ransom payments instead of prevention

Inclusion was screened for the first 40 Google Scholar results sorted according to their relevance. An additional review of cross-references in articles was performed to broaden the literature base.

2.3 PRISMA Flow

Figure 1 shows the selection process, summarised in a PRISMA style diagram.

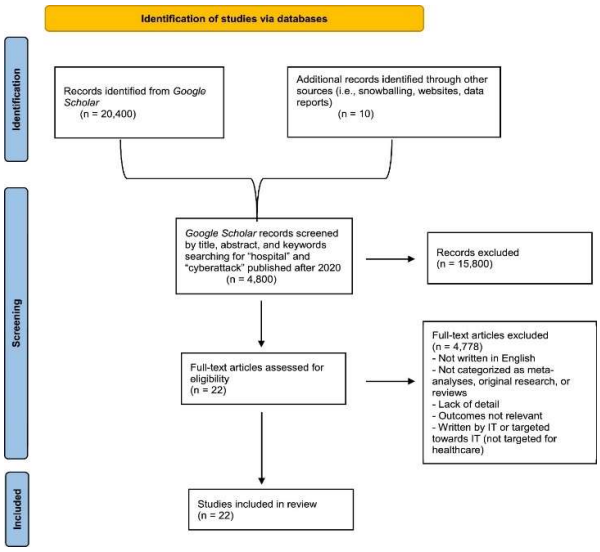

Figure 1: PRISMA flow diagram for systematic review

III. RESULTS

3.1 Growth of Cyber-Attacks in Healthcare (2009–2023)

According to the HIPAA Journal data (Alder, 2024) [2], healthcare cyber-attacks being reported have skyrocketed:

- **2018: 369 breaches**
- **2020: 663 breaches**
- **2023: 742 breaches**

This represents a doubling of incidents occurring from just 2018 into 2020, and an ongoing upward trend to 2023.

As of July 2024, there had already been 387 breaches of over 500 records. The number of patient records affected increased from:

- **April 2023: 5.2 million**
- **April 2024: 15.3 million**

That represents a threefold year-over-year increase.

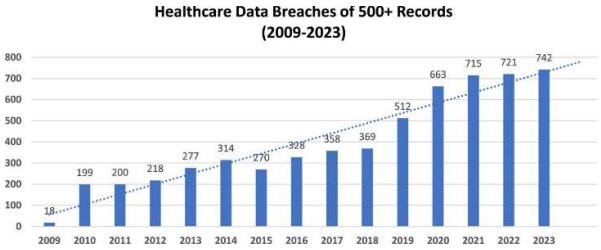

Figure 2: Number of healthcare data breaches from 2009–2023.

3.2 Case Example: Universal Health Services (UHS) Cyber-Attack

Admin, DRG Find the Top Cybersecurity Articles from 2021: 1.) One of the Largest U.S. Healthcare Ransomware Attacks Strikes Universal Health Services (UHS) in 2021 - Healthcare Cybersecurity Media - October 1, 2021 The attack resulted in:

- More than 4 weeks of scheduled EMR downtime
- Trauma and surgical case diversion
- Documentation for all inpatient services conducted manually
- Over $67 million in pretax losses, with forecast losses increasing above $113 million (Abbou et al., 2021) [12]

3.3 Common Types of Attacks

Table1 Summary of the prominent types of cyber-attack as outlined across reviewed literature (Shariff et al., 2021) [6]

TABLE 1. COMMON CYBER-ATTACK TYPES IN HEALTHCARE

Attack Type	Description	Impact
Phishing	Deceptive emails targeting staff credentials	EMR access compromise, unauthorized logins
Malware	Malicious code infecting systems	Operational disruption, data corruption
Ransomware	Encryption of critical systems demanding payment	EMR shutdown, diversion of patients
DoS / DDoS	Flooding servers to cause service outages	Telehealth failure, website shutdown

Figure 2: PRISMA Process

IV. RECOMMENDATIONS

4.1 Updating Legacy Systems

Nearly 85% of the Healthcare Organizations Are Operating Using Legacy Systems Like Windows XP Most of the Time they Do Not Do Security Patches (Ahmetoglu & Das, 2023) [9]. For instance, the British NHS was one of the organizations, with ~80,000 computers, which were affected by the 2017 WannaCry attack that compromised 200,000 systems across more than 150 countries, where a majority of the entry points were due to outdated devices.

4.2 Strengthening Medical Device Security

In the event of a cyber-attack, this could wreak havoc on medical devices like insulin pumps, ventilators, and MRI machines. In response, the FDA (2017) required:

- **Upgradable device software**
- **Built-in cybersecurity features**
- **A complete software bill of materials (SBOM)**

Hospitals should ensure that:

- **Device updates are aggregated and automatically applied**
- **Data transfer requires patient authorization**
- **Regular backups and digital signatures to validate device cleanliness**

4.3 Use of Blockchain and Network Segmentation

Segregating the network can help confine malware when it catches a strain of infection to only important systems. Sample EMR models such as MedRec and BlockHIE based on blockchain provide increased integrity of data by disseminating encrypted records across many decentralized nodes and avoiding a single point of failure.

4.4 Domain Protection Against Phishing

Buying up domain variations (e.g., more ". com" or ". Therefore, the domain name system change from "dot-com" to "dot-net" reduces the risk of phishing attacks in which the hospital's URL is spoofed (Rizzoni et al., 2022) [13].

V. LIMITATIONS

Google Scholar was the primary tool used for the systematic review, and while it has broad coverage, some peer-reviewed articles that met our inclusion criteria could have been missed due to the relevance-based ranking algorithm. The results from PubMed (which only returned a handful of results) highlight the general absence of biomedical-specific sources. It is therefore possible that not all literature published in less widespread journal outlets or hidden behind pay walls will be represented in the review.

VI. CONCLUSION

The realities of cyber-attacks on healthcare will continue to grow more sophisticated and more frequent, exposing the machinations of modern digital healthcare as a systemic weakness. The magnitude of an attack can create widespread operational disruptions, put significant financial pressure on hospitals, and increase safety risks to patients. A blend of the following is essential for achieving cybersecurity readiness:

- **Updated medical and IT systems**
- **Stronger threat-detection capabilities**
- **Staff training and cybersecurity awareness**
- **Secure medical device design**
- **Downtime protocols and recovery plans that can withstand stress**

In an ever-advancing digital landscape, an active, multi-layered security apparatus is needed to ensure clinical continuity and protection of sensitive patient information.

REFERENCES

[1]. L. Wasserman and Y. Wasserman, "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)," Frontiers in Digital Health, vol. 4, Art. 862221, 2022, doi: 10.3389/fdgth.2022.862221.

[2]. S. Alder, "Healthcare data breach statistics," HIPAA Journal, 2024. Accessed: Nov. 18, 2024.

[3]. Kroll, "The State of Cyber Defense: Diagnosing Cyber Threats in Healthcare", 2024.

[4]. https://www.kroll.com/en/insights/publications/cyber/state-cyber-defense-healthcare.

[5]. S. Z. Shariff, S. AD Bejaimal, J. M Sontrop, A. V Ivancevich's, R B. Haynes, M. A Weir, A. Garg, "Retrieving clinical evidence: A comparison of PubMed and Google Scholar for quick clinical searches", Vol. 15, Issue 8, 2013.

[6]. American Medical Association, Cybersecurity in Medical Practice, 2024.

[7]. **Kumar, R.** (2025, July–August). *Smart system, smarter world: A review of ML and DL innovation since 2018. International Journal for Multidisciplinary Research, 7*(4).

[8]. **Kumar, R.** (2025, April). *Adaptive cybersecurity with AI: Enhancing threat detection and response in intrusion detection systems. Indian Journal of Modern Research and Reviews.*

[9]. https://edhub.ama-assn.org/course/328

[10]. H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," Internet of Things*, 2022*.

[11]. S. Alder (Ed.), "Security breaches in healthcare in 2023," HIPAA Journal, 2024. https://www.hipaajournal.com/security-breaches-in-healthcare/

[12]. IBM, Cost of a Data Breach Report 2024. IBM Security, 2024. https://www.ibm.com/reports/data-breach

[13]. B. Abbou et al., "When all computers shut down: the clinical impact of a major cyber-attack on a general hospital," Front. Digit. Health, vol. 6, 16 Feb. 2024, Art. no. 1321485, doi: 10.3389/fdgth.2024.1321485.

[14]. G. Lippi and A. Ferrari, "Lessons learnt in medical laboratories during a disruptive cyber-attack," J. Lab. Precis. Med., vol. 9, Art. 18, 2024, doi: 10.21037/jlpm-23-84.

[15]. D. F. Sittig and H. Singh, “A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks,” Appl. Clin. Inform., vol. 7, no. 2, pp. 624–632, Jun. 2016, doi: 10.4338/ACI-2016-04-SOA-0064.

[16]. F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry, “Phishing simulation exercise in a large hospital: A case study,” Digit. Health, vol. 8, 2022, Art. no. 20552076221081716, doi: 10.1177/20552076221081716.

[17]. S. T. Argaw, J. R. Troncoso-Pastoriza, D. Lacey et al., “Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks,” BMC Med. Inform. Decis. Mak., vol. 20, art. 146, 2020, doi: 10.1186/s12911-020-01161-7.

[18]. The Big Phish: Cyberattacks against U.S. healthcare systems,” ScienceDirect, 2025. https://www.sciencedirect.com/science/article/pii/S2950386825000103

[19]. S. Gupta, Y. J. Singh and M. Kumar, "Object Detection Using Multiple Shape-Based Features", IEEE Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC 2016), pp. 433-437, December 2016.

[20]. S. Gupta, Y. Jayanta Singh, “Glowing Window Based Feature Extraction Technique for Object Detection”, International Conference on Data Management, Analytics and Innovation, New Delhi, 17-19 Jan, 2020.

[21]. S. Gupta, Y. Jayanta Singh, “Object Detection using Peak, Balanced Division Point and Shape Based Features”, 6th International Conference on Data Management, Analytics and Innovation, 14-16 Jan, 2022.

[22]. S. Gupta, H. Singh, Y. J. Singh, “Comprehensive Study on Edge Detection”, International Conference on Communication, Electronics and Digital Technology (NICE-2023), February 10-11 2023.