www.ijarp.com ISSN 2456-9992 Page: 01-06

International Journal Advanced Research Publications

Review Article

Volume: 02
Issue: 05

CYBERSECURITY IN HEALTHCARE SYSTEMS

***Patankar Hemlata Narendra, Shaikh Sabiya Latif, Mali Dipali Deepak**

Annasaheb Magar Mahavidyalaya, Hadapsar, Pune.

Article Received: 03 April 2026, Article Revised: 23 April 2026, Published on: 13 May 2026

***Corresponding Author: Patankar Hemlata Narendra**

Annasaheb Magar Mahavidyalaya, Hadapsar, Pune.

DOI: https://doi-doi.org/101555/ijarp.1949

ABSTRACT

The healthcare industry is really behind when it comes to keeping its data safe from cyber attacks. This is a problem because health data has a lot of sensitive personal and financial information. Cyber security incidents are becoming an bigger threat. To make things better we need to come up with a plan for finding the ways to deal with these issues. We need to look at the legal and social problems that come with using technology in healthcare like with telehealth and telemedicine. We also need to think about what we learned from the COVID-19 experience and see where we can improve. Then we can suggest some areas for research.

We found the information we needed by searching and looking at what other people have written about this topic. We also talked to experts. Looked at what professional organizations, like the EU have to say. We read nineteen papers and made categories to see what kind of ethical, legal and social issues they were talking about. We made a chart to help us keep track of all the issues that each source was addressing. The healthcare industry needs to take cyber-attacks and do something about it. Cyber-attacks are a deal and we need to find ways to stop them.

KEYWORDS: Cyber-attack, cybercrime, cybersecurity, cyber threats, health, healthcare, ransomware.

INTRODUCTION:

Cybersecurity is about keeping systems and networks, from bad people who want to hurt them. These people do things like try to get into our systems change our information or even destroy it. They also try to get money from us or stop us from doing our work. It is really hard to keep our systems safe because there are many devices connected to the internet and the bad people are always coming up with new ways to attack us. Cybersecurity is very

important because of this. We need to have cybersecurity to protect our systems and networks from these attacks. Cybersecurity is the way to keep our information safe. Cybercrime emerged in the late 1970 with the development of computer Information Technology.

Healthcare is an attractive target for cybercrime because it is a rich source of valuable data and not well protected. Cybersecurity breaches are a growing threat to the healthcare industry. The main objectives of this paper are to present a structured framework of eventual empirical research for linking Cyber Security improvement actions in healthcare systems to their strategic improvement needs. The structured framework is based on Quality Function Deployment (QFD), a generic, multi-purpose planning framework. The paper does not attempt to contribute to existing theories of cyber security or Quality Function Deployment.

LITERATURE REVIEW:

The healthcare sector is really worried about cybersecurity these days. This is because we are using a lot of technologies and electronic health records and we have many connected medical devices. Many people who study this topic say that healthcare organizations are very attractive to cybercriminals. This is because they have a lot of patient data.

According to Kevin Fu and other experts in cybersecurity the medical devices and hospital networks have vulnerabilities. These vulnerabilities can expose information and disrupt the healthcare services that patients need. (1)

There have been research studies about the impact of cyberattacks on healthcare systems. For example the WannaCry ransomware attack was very bad for hospitals. It locked access to data and systems which caused a lot of problems. Hospitals that were affected had to delay treatments cancel appointments. They had trouble accessing patient records. These incidents show that we need cybersecurity measures to protect our healthcare infrastructure. (2)

Other studies say that we need to implement security frameworks and policies to keep data safe. Researchers think that we should use data encryption, multi-factor authentication and regular system updates to reduce cybersecurity risks. We should also train employees on how to stay online. Organizations like the National Institute of Standards and Technology have proposed cybersecurity frameworks that can help healthcare institutions deal with cyber threats.

Cybersecurity in healthcare is also looking at technologies like artificial intelligence and blockchain. Artificial intelligence helps find activities in networks, which can stop cyberattacks. Blockchain technology gives a way to handle records. The literature shows that we need to mix technology, strong policies and healthcare professionals who are aware to

keep data safe. This will also ensure medical services keep going without any interruptions. Cybersecurity, in healthcare is crucial. We must take it seriously to safeguard healthcare organizations and patient data.

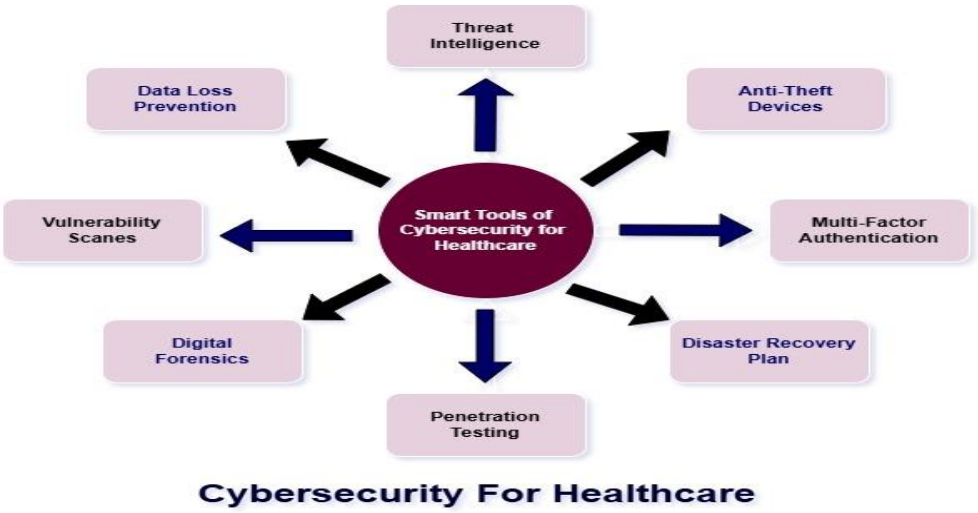

Figure 1: Smart tools of Cybersecurity in Healthcare.

RESEARCH METHODOLOGY:

This study looks at the problems that healthcare systems have with cybersecurity with cyber-attacks, cybercrime and ransomware threats. We did a review of what has been written about this topic in IEEE, PubMed and ScienceDirect using keywords like cyber-attack, cybercrime, cybersecurity, cyber threats, health, healthcare and ransomware. We studied how to protect healthcare systems from cyber threats. We focused on keeping Electronic Health Records and medical devices safe. (3)

There are some cyber threats that we found like ransomware attacks that stop healthcare services from working and phishing that gets sensitive data. What we learned shows that healthcare systems need to have cybersecurity measures in place like encrypting data separating networks and training staff. Using intelligence to detect threats can make healthcare cybersecurity better. Healthcare organizations must make cybersecurity a priority to prevent data breaches and keep patients safe. (4)

In the future researchers should work on creating cybersecurity plans that are tailored to healthcare organizations. They should address problems, like not having enough resources and using old systems. It is very important for healthcare providers and cybersecurity experts to work together. By making cybersecurity stronger healthcare systems can reduce risks. Keep people's trust.

Table 1: Sample Data. (2020-2025 Summary)

Year	No. of Incidents	Most Common Attack	Avg. Records Compromised	Avg. Recovery Time (days)
2020	550	Ransomware (COVID-19 healthcare targeting)	8-10million	~280
2021	650	Ransomware + phishing cyber-attacks	10-12 million	~300
2022	750	Ransomware (dominant healthcare cybercrime)	12-14 million	~290
2023	1,200+	Phishing	45,000avg per breach	~277-326
2024	677+	Ransomware (healthcare most targeted sector)	182 million	~30-300
2025	1,100+	Advanced ransomware + AI-driven cyber threats	15-20 million+	~23-250

Table 2: Year-Wise Summary of Cybersecurity Incidents.

Year	No. of Breaches (approx.)	Records Compromised (millions)	Avg. Recovery Time (days)
2020	550	8-10	280
2021	650	10-12	300+
2022	750	12-14	290
2023	1,200+	0.045	277-326
2024	677+	182	30-300
2025	1,100	15-20	23-250

CHALLENGES & OPEN ISSUES:

Challenges

- Ransomware attacks disrupt healthcare services.
- Budget for cybersecurity is limited in healthcare.
- Such systems are susceptible to cyber-attacks.
- Thwarting cybercrime against health data isn't easy.
- Staff lack cybersecurity training.
- Wearable Shift in Health Care: Device to wear and tear

Open Issues

- Standardized Cybersecurity Frameworks for Healthcare is Necessary
- AI can improve healthcare cybersecurity.
- Better cybersecurity is based on collaboration.
- It's a delicate balancing act, compliance versus threats from cyber warfare.
- Patients need awareness about cybersecurity.

- We need to deal with cyber threats, in healthcare as they come up.

RESULT:

The results of this research indicate that the healthcare sector has become one of the most vulnerable areas to cyber-attacks and cybercrime due to the rapid adoption of digital technologies and the storage of highly sensitive patient data. The study found a significant rise in cyber threats, including malware, phishing, and especially ransomware attacks, which have severely impacted hospitals and medical institutions. In many cases, ransomware has locked critical patient records and demanded payment, leading to delays in treatment and negatively affecting patient health outcomes.

Furthermore, the research highlights that many healthcare organizations still lack strong cybersecurity measures. Weak system infrastructure, outdated software, and insufficient staff awareness make it easier for attackers to exploit vulnerabilities. Data breaches were also identified as a major issue, where confidential patient information is stolen or misused, resulting in loss of trust in the healthcare system.

The findings also reveal that cyber incidents not only cause financial losses but directly disrupt medical services, including diagnosis, treatment, and emergency care. Overall, the study concludes that without robust cybersecurity strategies, continuous monitoring, and proper training, the risk of cyber threats in healthcare will continue to grow, posing serious challenges to both patient safety and the efficiency of healthcare services.

CONCLUSION:

So healthcare systems are really important. We need to protect them from cyber attacks. Cybercrime and ransomware are risks. We have to keep health records safe. We also have to protect the machines doctors use. These records and machines have a lot of information. We do not want this information to fall into the hands.

Here are some ways to keep healthcare systems safe:

* We can use encryption to protect information.

* We can use security measures to keep the network safe from cyber attacks.

This will help prevent cyber attacks. Healthcare organizations must do everything they can to keep information safe. They also need to make sure patients are safe and healthy.

There are cyber threats out there. They are getting worse every day. We need to be proactive and work on keeping healthcare systems safe. Healthcare workers and cybersecurity experts

must work together. If they do we can keep patients safe. We can also keep their health information safe and secure.

As we use computers and digital systems in healthcare we need to make sure they are safe and secure. This is really important for patients. We want to keep taking care of patients. We want to make sure they get the care they need and deserve. Some problems need to be fixed away. One problem is not having money. Another problem is systems that're not safe. If we improve cybersecurity we can reduce the risks. This will help keep healthcare systems from cyber threats. Patients will be safe. They will also trust the healthcare system. Healthcare systems are really important for our society. They need to be safe, from cyber attacks.

REFERENCES:

1. Fu, Kevin (2019). Security challenges in medical device software. 62(10), 44–49, Communications of the ACM
2. Radanliev, Petar, De Roure, D., Nicolescu, R., and Huth, M. (2020). Cyber risk analytics in healthcare systems. 10, 1–12, Journal of Cybersecurity.
3. Jalali, M. S., and Kaiser, J. P. (2018). cyber security in hospitals: a systematic, organizational perspective. 6, 8791-8805, IEEE Access.
4. Sarker, I. H. (2021). ai-based cybersecurity: a comprehensive review. 10(2), 1-17, Journal of Cybersecurity and Privacy.