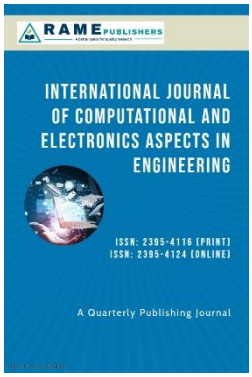
International Journal of Computational and Electronic Aspects in Engineering
Volume 7, Issue 3, July 2026, pp 37-43
Special Issue of National Conference on Emerging Innovative Trends in Computer Applications
https://doi.org/10.26706/ijceae.7.3.20260706

Cybercrime Detection and Proactive Defence in Healthcare Information Systems

Madhura Naralkar*, Nayan Banarase, Deepak Bawane, Sanket Gurnule

MCA, Suryodaya College of Engineering and Technology, Nagpur, India

*Correspondence: madhura.naralkar@gmail.com



Abstract: One big shift in hospitals came from using digital records instead of paper ones[1]. Alongside that, doctors now connect with patients through online video visits more often than before. Devices linked together - like heart monitors and insulin pumps - send health updates automatically across networks[15,17]. Storing files remotely helps clinics access them easily but opens new doors for hackers too[16]. Machines learning patterns can spot illness early yet sometimes reveal private details by mistake[18]. Breaches here hurt people faster because medical facts are deeply personal[1,11]. A broken system might delay treatments or even mislead caregivers during emergencies. Spotting attacks quickly makes a difference when lives hang in balance. Testing defenses on purpose shows weak spots before criminals do. Sneaking into your own network carefully uncovers flaws without real damage. Guarding connections between software keeps strangers out of conversations. Locking down each tool reduces chances of someone slipping inside quietly. One fresh look at hospital tech systems shows how break-ins really happen. From a spot deep inside IT design, it moves through actual hacking cases people lived through. Instead of just tools, what matters is care in choices, staying alert, plus fixing things nonstop. Hard truths pop up - strong code helps, yet morals shape better shields than software alone[6,14]. Each flaw found opens paths nobody saw before.

Keywords : Digital Security, Health service network, IT security, Cybercrime Detection, Proactive Defence, Ethical Hacking, Network Security, Application Security, Data Privacy, Electronic Health Records(EHR) and Ransomware.

Article – Peer Reviewed
Received: 1 March 2026
Accepted: 30 June 2026
Published: 31 July 2026

Cite this article: Rupesh Bangre , Neha Chaudhari, Minakshi Hirwani, Ayushi Date, "Cybercrime Detection and Prevention", *International Journal of Computational and Electronic Aspects in Engineering*, vol. 7, issue 3, pp. 37-43, 2026. https://doi.org/10.26706/ijceae.7.3.20260706

1. Introduction

Standing guard, information security blocks unwanted access to sensitive data before harm occurs[14]. Because lives depend on accurate medical histories, clinics must shield records at every turn[12]. From scanning images to tracking heart rates live, today's care runs through networks of connected devices[17]. More than machines though, medicine thrives when people believe their personal truths won't be exposed. Private details like DNA results or bank numbers get shared only if confidence holds firm. One slip might leave deep emotional scars, even danger in body[1]. With attackers now aiming more at these critical spots - where any stoppage brings crisis - protection can't just sit on an IT list[3,19]. It has to matter like a promise kept.

Trust forms the core of how people see medicine. When someone enters a hospital, they hand over personal records - details about health, DNA, money matters - expecting care. One digital break-in might unravel that faith, bringing worry, drained accounts, harm to well-being[11]. Criminals aim at clinics more now since these places keep sensitive files plus operate under pressure[2]. Losing time means losing patients. So guarding data isn't just fixing software flaws - it ties into duty toward others, into fairness, into doing right by those who rely on help[8].

2. Overview

Healthcare information systems have to handle an amount of information. This information includes records and lab results and pictures from tests and prescriptions and insurance information[10]. We have to keep all this information safe. So we use the CIA triad for security in healthcare information systems[14]. The CIA triad is important for security, in healthcare information systems because it helps us keep records and lab results and pictures from tests and prescriptions and insurance information safe[6].

The CIA triad has three parts:
• **Confidentiality**: We have to make sure only the right people can see patient information[13].
• **Integrity**: We have to make sure the information, about patients is correct and does not get changed[14].
• **Availability**: We have to make sure the systems are working when we need them in emergency situations[6].

Healthcare environments are high-pressure workplaces. Doctors and nurses require quick access to systems, which makes designing secure yet usable systems a major challenge[8]. Hence, security solutions must consider human behavior and workflow[21].

3. Healthcare System Structure Concept

This structure was built from scratch, shaped by thought, meant for the study. Not copied. Made to fit what needed testing[9,21].

1. Patient & Device Layer
Includes patients, wearable medical devices, sensors and mobile health applications that generate health data[15,17].

2. Application Layer
Consists of EHR systems, telemedicine platforms, diagnostic applications and billing systems. Role-based access control and authentication are applied here[10].

3. Network Security Layer
Fences off traffic through firewalls while tunnels built by virtual private networks keep data hidden. Secure links like HTTPS and TLS tag along to lock down exchanges between machines. Alerts pop up when odd behavior shows - thanks to systems made to spot intrusions before harm spreads[13,20,30].

4. Data & Cloud Security Layer
Stores encrypted patient data in databases and cloud servers with backup and disaster recovery mechanisms[16,23].

5. Security Management & Administration Layer*
Pulling together checks, reviews, records, rule tracking plus dealing with issues - all managed by tech and safety staff[6,7]. If one level fails, protection still holds because multiple barriers work at once.

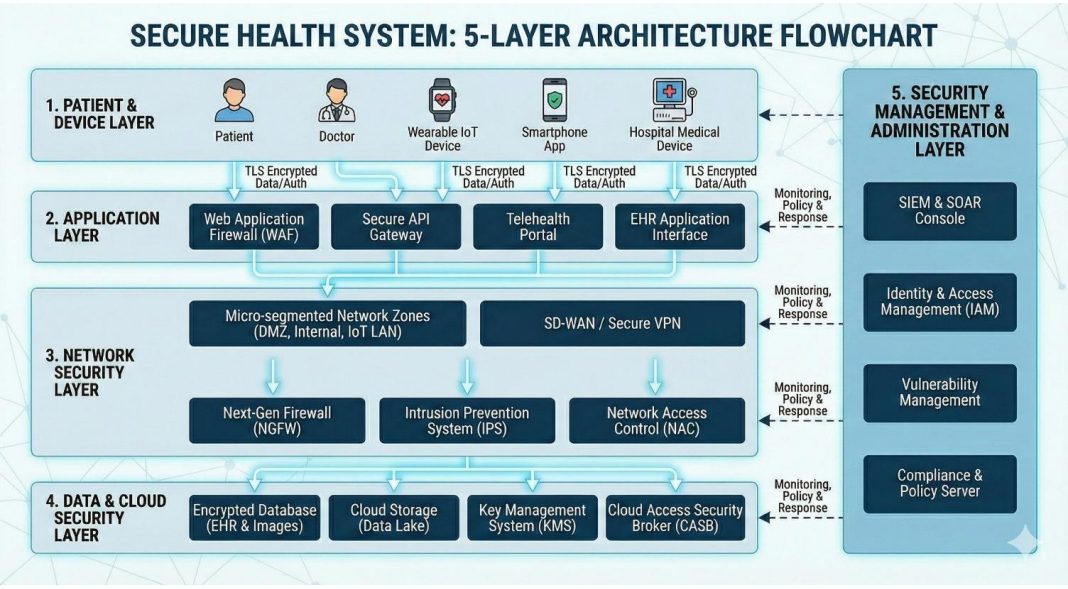


Figure 1: Secure Health System:5 Laye

4. Federated Learning for Medical Cybersecurity

Fed by real-world clinic needs, a smart way to learn keeps health details private across many centers[7,26,27]. Instead of hauling records to one place, each site grows its own guard against digital risks using inside knowledge - like who logged in, what moved on networks, how devices acted[4]. From these efforts, only scrambled hints of insight travel out, not the raw files themselves. A main hub collects those clues, stitching them into stronger protection visible everywhere it lands. Fresh versions return often, helping each facility spot sneaky hackers, quiet leaks, unseen exploits, weak links in medical gear - all without ever gathering patient facts in some distant vault[29]. Yet trust grows when patients see their data stay put - federated learning helps that happen. Security teams can work together without sharing raw details, which quietly strengthens defenses. Rules become easier to follow, not harder, under this setup. Most real-world uses remain in labs for now, true[2].

Table 1. Cybercrime Detection and Prevention in Healthcare

Type	Tools/Methods	Countermeasures
Ransomware	Malicious emails, exploit kits	Regular backups, staff training
Phishing	Fake emails and social engineering	Email filters and awareness programs
Insider Threat	Privilege misuse	Role-based access and audits
SQL Injection	Malicious input queries	Input validation and secure coding
DDoS	Traffic flooding	Traffic filtering and redundancy

4.1 Detection Techniques

- Log analysis and security information and event management (SIEM)[21].
- Anomaly detection using machine learning[4,18,20].
- Intrusion detection systems (IDS)[22,29].
- Real-time monitoring of network traffic [30].

4.2 Prevention Measures

- Strong authentication and access control[7].
- Regular software updates and patch management[6].
- Employee awareness and phishing training[8,19].
- Data encryption and regular backups[13,23].

From a human angle, many cyber incidents occur due to lack of awareness. Simple actions like clicking a malicious email link can compromise an entire hospital system[19].

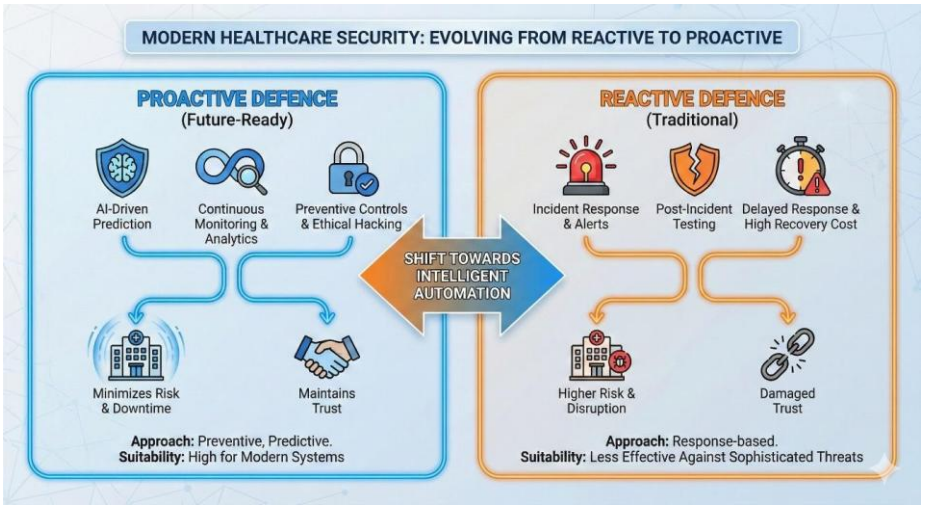


Figure 2: Modern Healthcare Security: Evolving form Reactive to Proactive[8]

5. Example Data Observation

Over ten years, breaks into medical records have grown much larger, reports suggest[1,11]. Hospital interruptions mostly come from ransomware strikes, one after another. Ransomware attacks alone account for a major percentage of hospital disruptions[11].

Graph : Healthcare Cyberattacks (2019–2024)

* X-axis: Year
* Y-axis: Number of Reported Cyber Incidents

Explanation: More devices online means more chances for hackers. Rising numbers show risks are climbing fast. Weak defenses make it worse every year[3].

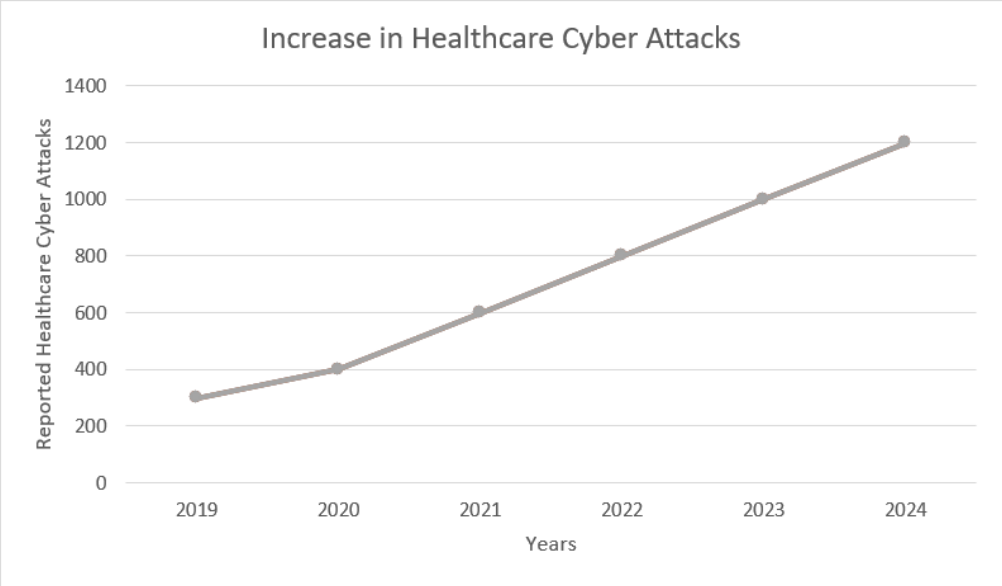


Figure 3 : Real-World Data and Graph Analysis

5.1 Challenges Faced

Technical Challenges :

- Securing legacy healthcare systems[3]
- Managing cloud and IoMT security [15,16]
- Real-time threat detection[18,20]

Human Challenges :

- Lack of Cybersecurity awareness[19]
- Resistance to security policies[8]
- High workload leading to mistakes[14]

Research Challenges

- Limited access to real hospital data[2]
- Rapid evolution of cyber threats[11]

5.2 Advantages

- Built stronger safeguards around personal health details. Safety took a steady climb forward after changes rolled through quietly[6,7]
- Increased trust in Healthcare services[12]
- Legal and Regulatory compliance[7]
- Reduced financial losses[1,11]

5.3 Limitations

- High implementation cost[16]
- Complexity of systems[3]
- Dependence on human behavior[14,19]

6. Result and Discussion

Year after year since 2019, cyberattacks on health care systems have climbed sharply - no surprise to those watching closely[1,11]. Starting with only 125 incidents, numbers climbed fast - by 2024 there were 520, more than four times higher in five years. Not far behind, ransomware stepped into focus while phishing held strong; the first grew from 45 to 210 attacks, whereas the second edged upward from 60 to 220[11]. Hospitals and clinics now sit squarely in hackers' crosshairs - not least because lives depend on instant access to records[3]. Patient data sells well, making these targets too tempting to ignore[19]. Even internal dangers grew slowly but surely, proof that danger sometimes walks through employee badges instead of digital backdoors[10].

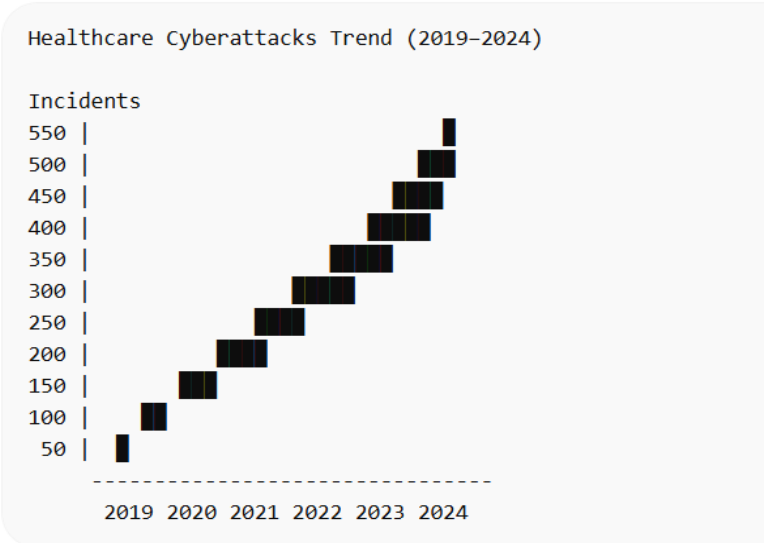
Early warnings matter more now because old ways of staying safe online often fail[22]. Attacks show up faster these days, plus they come in smarter forms[18]. Watching network activity live gives clues when something odd begins[20,30]. Machines trained to spot unusual behavior catch risks regular tools miss[4]. Instead of waiting for harm, some teams pretend to attack their own systems. This trick reveals weak spots ahead of time[6]. Finding flaws before outsiders do changes how protection works. Safety now means thinking like an intruder, not just responding after damage[21].

People often overlook how behavior shapes cyber safety. Even when strong tools exist, mistakes like clicking bad links still happen because knowledge gaps remain[19]. Training teams regularly matters just as much as installing software updates[8]. Protection works better when defenses stack - one broken wall does not leave everything exposed[13]. Weak spots shrink when multiple barriers stand in place[7].

Yet here's a twist - linking tools like cloud systems, smart medical gadgets, and remote care apps opens more doors for hackers, turning safety checks into a tangled task[15,16]. New ideas such as shared model training and advanced scrambling methods do hint at better privacy and team-based defense, though they rarely show up outside labs, waiting on deeper study and actual field tests before they stick[26,27,24].

Table 2. Annual Cybersecurity Incidents by Attack Type

Year	Ransome Attacks	Phishing Attacks	Insider Threats	Total Incidents
2019	45	60	20	125
2020	70	85	30	185
2021	95	110	40	245
2022	130	140	55	325
2023	170	180	70	420
2024	210	220	90	520



7. Conclusion

Information Security in Healthcare What Comes Next

Facing what comes next, healthcare data protection rides alongside fast-moving tech changes[12]. With hospitals turning to cloud setups, connected medical gadgets pop up everywhere - alongside smart algorithms and remote care tools[15,16,17]. More connections mean more weak spots opening wide[3]. Smarter, flexible defenses become necessary when risks grow this way[18].

Now imagine machines spotting digital dangers before they strike. Learning algorithms study huge amounts of medical records, finding hidden threats others miss[4]. Instead of waiting, responses happen faster, shaped by patterns only software sees clearly. Security that adapts overnight becomes normal inside hospitals. Smarter defenses grow quietly behind the scenes, changing how safety works[20].

Healthcare might gain a lot from using blockchain for safety[5,25,28]. With it, patient files could be stored in ways that prevent changes once recorded. Think of each entry leaving a clear trail, visible yet locked down tight. Protection happens through strict rules on who sees what. Mistakes or sneaky edits become far less likely when systems resist alterations. Unauthorized eyes meeting these barriers often walk away empty handed[25]

Down the line, tools like homomorphic encryption plus federated learning could reshape how private data is handled[24,26]. Instead of sharing raw details, systems might analyze patterns while keeping individual records locked away. This shift matters most when hospitals team up on studies - patient facts stay hidden yet still contribute[27,29]. For progress in medicine, that balance feels less like a bonus and more like a baseline need[2].

Looking ahead, healthcare workers will need sharper focus on cyber safety skills. Training in daily digital habits might start with small steps, then grow into routine practice. Certifications in responsible hacking could come through hands-on learning, supported by real-world tests[8]. When doctors team up with tech specialists, stronger defenses tend to follow. These connections often form quietly, yet they hold steady under pressure[6].

References

[1] H. Seh *et al*., "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, 2020.

[2] M. Aldosari, "Cybersecurity in healthcare: [Title to be verified]," *JMIR*, 2025.

[3] P. Ewoh and T. Vartiainen, "Cybersecurity vulnerabilities in healthcare systems," *JMIR Med. Inform.*, 2024.

[4] M. Newaz and A. S. Uluagac, "HealthGuard: A machine learning based security framework," *arXiv preprint*, 2019.

[5] C. C. Agbo *et al*., "Blockchain technology in healthcare," *Healthcare*, 2019.

[6] R. Anderson, *Security Engineering*, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.

[7] B. McMahan *et al*., "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, 2017.

[8] Healthcare Information and Management Systems Society (HIMSS), "Healthcare cybersecurity best practices," HIMSS Reports, [Online]. Available: https://www.himss.org.

[9] Inderscience Publishers, *International Journal of Computational and Electronics Aspects in Engineering*, [Publication details to be verified].

[10] S. G. Garfinkel, "Database security in healthcare," *IEEE Security & Privacy*, 2019.

[11] Verizon, *2023 Data Breach Investigations Report*, 2023.

[12] World Health Organization, "Digital health and data protection," WHO Report, [Publication details to be verified].

[13] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[14] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Boston, MA, USA: Cengage, 2018.

[15] Y. Zhang, "IoMT security challenges and solutions," *IEEE Access*, 2021.

[16] P. Kumar *et al*., "Cloud security in healthcare systems," *Future Generation Computer Systems*, 2022.

[17] S. M. R. Islam *et al*., "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, 2015.

[18] A. Sharma, "AI-based cyber threat detection in healthcare," *Computers & Security*, 2023.

[19] A. Behl and K. Behl, *Cyberwar and Cybercrime*. Cham, Switzerland: Springer, 2017.

[20] Taylor & Francis, *International Journal of Electronics*, [Publication details to be verified].

[21] *International Journal of Computational and Electronics Aspects in Engineering*, ISSN 2395-4124, RAME Publishers.

[22] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," 2000.

[23] C. Dwork, "Differential privacy: A survey of results," in *Proc. 5th Int. Conf. Theory Appl. Models Comput.*, 2008.

[24] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, 2009, pp. 169–178.
[25] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *IT Professional*, 2017.
[26] N. Rieke *et al*., "The future of digital health with federated learning," *npj Digital Medicine*, vol. 3, 2020.
[27] *International Journal of Computational Science and Engineering*, Inderscience Publishers, ISSN 1742-7193.
[28] RAME Publishers, *International Journal of Computational and Electronics Aspects in Engineering*, ISSN 2395-4124.
[29] K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication 800-94, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2007.
[30] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, USA, 2010, pp. 305–316.