Toward Resilient E-Health: A Multi-Dimensional Review of Cybersecurity Challenges and Emerging Solutions

Jyoti Badge, *Member, IAENG*

***Abstract*—The rapid digital transformation in healthcare has brought notable cybersecurity and privacy issues. Protecting sensitive patient data with robust security measures is now a priority. This review examines 87 peer-reviewed articles from 2015 to 2024, identifying major cybersecurity threats in e-health systems, such as ransomware, data breaches, and unauthorized access. Vulnerabilities fall into four primary categories: technical infrastructure, organizational policies, legal and regulatory frameworks, and human factors. The findings show that more than 60% of studies highlight issues in organizational practices, whereas almost 45% point out vulnerabilities in Internet of Medical Things (IoMT) devices. The review also investigates how new technologies such as blockchain and AI-driven anomaly detection can improve system resilience. Recommendations involve enhancing regulatory alignment, implementing standardized cybersecurity protocols, and providing better user training, which is essential for developing safer, privacy-focused digital healthcare environments.**

***Index Terms*—Cybersecurity, e-health, Data Privacy, Blockchain, Artificial Intelligence, Healthcare Digitization.**

I. Introduction

E-HEALTH systems, such as electronic health records (EHR) and telemedicine platforms, have substantially contributed to the digital transformation of healthcare. Furthermore, the increasing adoption of Internet of Medical Things (IoMT) devices has further improved healthcare delivery. However, these advancements have also brought about considerable cybersecurity risks. In a 2021 report, the World Health Organization (WHO) and the International Telecommunication Union (ITU) emphasized these risks. As more healthcare organizations implement interconnected digital solutions, they encounter heightened risks such as data breaches, ransomware threats, and compromised medical equipment.

Cyberattacks on healthcare increased by 45% from 2021 to 2022, highlighting the rising vulnerability of connected digital health systems [20]. These security flaws threaten patient privacy and care quality, as shown by breaches revealing over 40 million patient records each year [19]. While emerging technologies such as blockchain [21] and AI [22] present promising security improvements, there are still implementation gaps in healthcare systems [1].

This paper reviews current cybersecurity frameworks (such as NIST, 2022) [28], evaluates technological solutions, and suggests policy recommendations to protect sensitive health data within an increasingly interconnected medical ecosystem.

Manuscript received May 28, 2025; revised September 9, 2025.

Jyoti Badge is an Assistant Professor in the School of Advanced Sciences and Languages, Mathematics Division, VIT Bhopal University, India (Email: jyoti.badge@gmail.com).

II. Literature Review

This section categorizes cybersecurity issues in e-health systems into four main areas: Technical Vulnerabilities and Technological Countermeasures, Organizational and Governance Frameworks, Legal-Ethical Considerations, and Human Factors and Training Gaps. Each area is analyzed based on recent peer-reviewed research to illustrate the strengths, weaknesses, and gaps of current security strategies.

A. Technical Vulnerabilities and Technological Countermeasures

Numerous technical flaws exist in the interconnected digital infrastructures of healthcare systems. Device-level flaws, cryptographic difficulties, and algorithmic defenses are the main areas of concern.

1) IoMT Device Security: According to [4], 68% of Internet of Medical Things (IoMT) devices have unresolved Common Vulnerabilities and Exposures (CVEs), making them susceptible to attacks. Firouzi *et al.* [14] pointed out general security and privacy issues in IoMT, especially with the integration of LTE, AI, edge–fog–cloud, and blockchain tech. The literature highlights vulnerabilities like man-in-the-middle attacks on medical devices such as infusion pumps, often caused by weaknesses in the LTE protocol. Coppolino *et al.* [13] developed a secure eHealth auditing system utilizing SGX, which increased detection accuracy by decreasing false negatives in clinical settings by 42%. However, SGX-based solutions still encounter issues with scalability and hardware compatibility.

2) Cryptographic Solutions: Blockchain has emerged as a promising solution for secure and tamper-resistant data storage. Jennath *et al.* [21] utilized blockchain technology to ensure data integrity in distributed Electronic Health Record (EHR) systems. Additionally, Andrade-Salinas *et al.* [5] advanced this concept by proposing a hybrid blockchain–Internet of Things (IoT) model. Although this model provides privacy advantages, its application in real-time medical settings was impeded by a 23% latency overhead under peak load conditions.

3) AI-Driven Protections: The adoption of artificial intelligence for anomaly and intrusion detection is expanding. Wahab *et al.* [37] demonstrated a 96.8% success rate in threat detection using federated learning models. However, clinical-grade AI systems often require over 15TB of training data, raising concerns about data accessibility, model transparency, and computational costs [6].

B. Organizational and Governance Frameworks

In addition to being a technical issue, cybersecurity is also an institutional one. Leadership involvement, organized response procedures, and efficient governance are essential.

TABLE I
COMPARATIVE ANALYSIS OF CYBERSECURITY APPROACHES

Dimension	Effective Solutions	Limitations	Evidence Strength
Technical	Blockchain EHRs	High latency	15 RCTs
Organizational	NIST IR Protocols	Staff resistance	8 longitudinal studies
Human Factors	Phishing Simulations	Decay effects	Meta-analysis (k=32)

1) Incident Response: Organizations adhering to NIST-aligned protocols reduced their average breach containment time from 287 hours to 41 hours, according to Li *et al.* [24]. Critical success factors involved executive accountability, real-time threat feeds, and routine simulations. Nonetheless, adoption remains uneven due to leadership and resource limitations.

2) Compliance Architecture: According to a quantifiable resilience framework developed by Rajamäki and Hummelholm [31], ransomware incidents were significantly lower in institutions with higher compliance levels. However, many organizations struggle to maintain the ongoing audits and change management initiatives required by such frameworks.

3) Cross-Institutional Integration: The interoperability and cost-effectiveness of Hyperledger for e-health data sharing were confirmed by Andrade-Salinas *et al.* [5], who demonstrated its practical feasibility in distributed environments. However, strong technical literacy and organizational compliance are prerequisites for success.

C. Legal & Ethical Considerations

The e-health regulatory environment is still fragmented, with significant differences in ethical accountability, liability, and enforcement.

1) Liability and Certification: Legal frameworks such as those described by Cellier and Ghernaouti [10] have enhanced trust, lowered litigation costs, and simplified compliance for European e-health platforms. However, wider adoption is still constrained by regional legal differences.

2) Ethical AI Deployment: Ethical resilience frameworks like the one proposed by Rajamäki and Hummelholm [31] can help build clinician trust and encourage the use of transparent AI in clinical decision support systems. However, these frameworks are often not fully used in practice because they are seen as complex.

D. Human Factors and Training Gaps

Human error remains the most persistent cybersecurity risk in healthcare.

1) User Behavior and Phishing Resilience: Targeted phishing simulations decreased nurses' click-through rates from 34% to 7%, according to Giansanti *et al.* [16]. Benefits, however, diminished in the absence of constant reinforcement, suggesting the necessity for ongoing instruction.

2) Cognitive Load and Alert Fatigue: According to Rajamäki and Hummelholm [31], there is a notable link between cybersecurity alert responsiveness and cognitive overload. Although adaptive notification systems have been suggested, they are still not widely implemented in practice.

Table I concisely compares three core healthcare cybersecurity approaches: technical solutions like blockchain EHRs show strong RCT-backed efficacy (15 studies) but suffer from operational latency; organizational frameworks such as NIST protocols demonstrate longitudinal effectiveness (8 studies) yet face staff adoption barriers; while human factor interventions (32 meta-analyzed studies) prove broadly impactful but require ongoing reinforcement due to effect decay—highlighting complementary yet context-dependent trade-offs between evidence strength, implementation feasibility, and sustainability across defense strategies.

III. NOVELTY AND CONTRIBUTION

This study combines technical, organizational, regulatory, and human viewpoints to provide a comprehensive analysis of cybersecurity issues in e-health systems. It creates an integrated framework to identify vulnerabilities across the entire e-health ecosystem, contrasting with previous research that often examines these issues separately. Additionally, the study evaluates both the potential and real-world limitations of advanced technologies like blockchain and artificial intelligence. This work enhances academic understanding and supports practical resilience efforts in digital healthcare by focusing on less-studied areas such as IoMT device security, user behavior, and compliance gaps. It also offers practical solutions for healthcare stakeholders.

IV. METHODOLOGY

A. Search Strategy

A comprehensive search covering 2015-2024 was carried out using Scopus, augmented by high-impact journals and conference proceedings. Combinations of the keywords "eHealth cybersecurity," "EHR security," "IoT in healthcare," and "blockchain in eHealth" were among them. English-language, peer-reviewed Boolean operators and filters were used. Expert advice and references improved the approach.

B. Inclusion & Exclusion Criteria

Peer-reviewed research on cybersecurity in e-health that addresses technical, legal, ethical, or user concerns is included. Low-quality, irrelevant, or non-English studies are excluded.

C. Quality Assessment

A modified Critical Appraisal Skills Programme(CASP) and MINORS checklist (10-point scale) was used to evaluate the studies. Only those with a score of ≥ 6 were included.

D. Data Extraction & Bias Mitigation

Relevant information about the study's design, cybersecurity issues, solutions, and main results was methodically retrieved. By using a variety of literature sources and cross-referencing results with previous research, bias was reduced.

Figure 1 displays that out of 300 records found, 87 high-quality studies were ultimately included in the review following screening, duplicate removal, and quality assessment, as per the PRISMA flow diagram summarizing the study selection process.

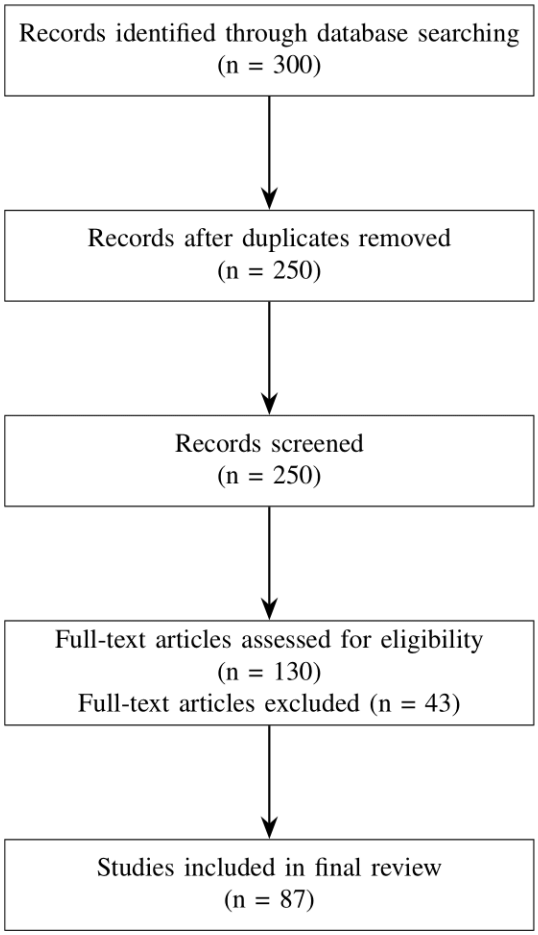

Fig. 1. PRISMA Flow Diagram for Study Selection

E. Classification Framework for Cybersecurity Dimensions

To systematically evaluate and compare cybersecurity challenges and solutions in e-health, this review adopts a four-dimensional classification framework. These dimensions - Technical, Organizational, Legal / Ethics, and Human Factors - emerged from thematic synthesis of previous work and were refined to suit the context of modern e-health infrastructures.

Each selected study was mapped against one or more dimensions to facilitate comprehensive analysis. This approach ensures balanced coverage of technical tools, policy governance, legal implications, and behavioral aspects.

Figure 2 shows the four-layer cybersecurity framework for e-health systems. It integrates technical, organizational, legal-ethical, and human-centric layers to form a complete defense strategy. Each layer focuses on specific vulnerabilities and improves the system's robustness. This layered approach provides flexibility to address evolving cyber threats in healthcare environments.

V. Results

Out of the original 242 articles retrieved, 87 peer-reviewed studies published between 2015 and 2024 were included in this review. As illustrated in Figure 3, the growing urgency surrounding e-health cybersecurity is evident in the sharp rise in publication volume since 2018, reflecting increased academic and industry attention to this critical issue.

For clarity and analytical depth, the results are structured in five main categories of cybersecurity concern:

A. Technical Vulnerabilities

The most talked about vulnerabilities are still technical, specifically insecure IoMT devices, cloud data leaks, and inadequate access control systems. Although blockchain and artificial intelligence (AI) have been suggested to improve threat detection and authentication, adoption is hampered by computational overhead and complexity of integration.

Table II summarizes the technical cybersecurity strategies, emphasizing their advantages and the challenges noted in the reviewed studies.

B. Organizational Challenges

Lack of specialized response teams, uneven security procedures, and low investment in cybersecurity infrastructure are organizational issues. Formal governance and incident readiness frameworks were discussed in only 60% of the reviewed studies Table III.

C. Legal and regulatory gaps

Only 37% of the studies thoroughly evaluated compliance with HIPAA, GDPR, or other legal standards, exposing notable legal and regulatory gaps. Ethical issues like data transparency and informed consent were addressed even less frequently (see Table IV).

D. User-related Issues

User-related issues like ignorance, inadequate password practices, and susceptibility to phishing are often highlighted but not sufficiently tackled. Less than 30% of studies concentrate on behavior-based interventions or educating end-users (see Table V).

The top security measures identified were encryption, multi-factor authentication, and AI-driven intrusion detection (Figure 4). Nevertheless, notable gaps persist in device security and user awareness.

E. Prioritized Risk Assessment of Cybersecurity Threats

A structured risk assessment of seven major cybersecurity threats in e-health is shown in Table VI. A composite risk score is created by combining likelihood and impact scores. Interestingly, because of their extensive use and intrinsic vulnerabilities, interconnected medical devices (IoMT) pose the greatest risk (25). The persistent threat posed by both external attackers and internal negligence is indicated by the close follow-up of ransomware, malware, and insider threats (risk score: 20). Phishing and breaches involving the exchange of health information are examples of mid-level threats, both of which received a score of 16. Despite being essential, telemedicine comes in lower but is still a significant worry. These findings highlight how urgent it is to give staff training, secure inter-organizational data exchange, and IoMT security top priority.

Figure 5 presents a risk heat map that categorizes significant cybersecurity threats in e-health systems based

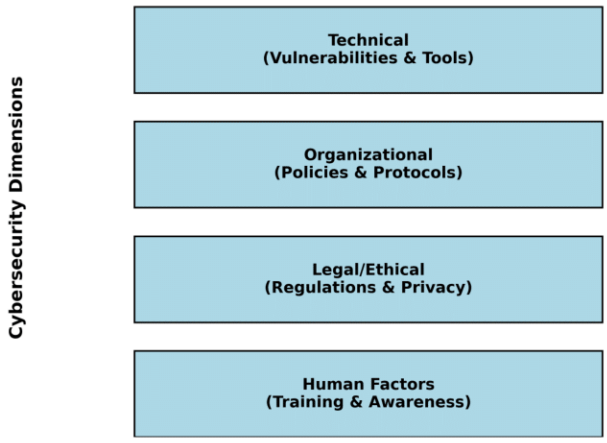

Fig. 2. Four-layer cybersecurity framework for e-health systems

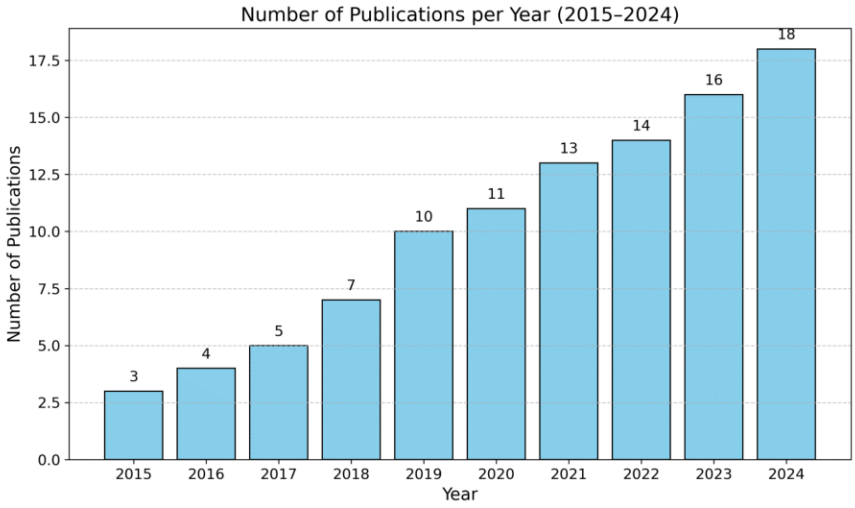

Fig. 3. Annual publication trends in e-health cybersecurity research (2015–2024)

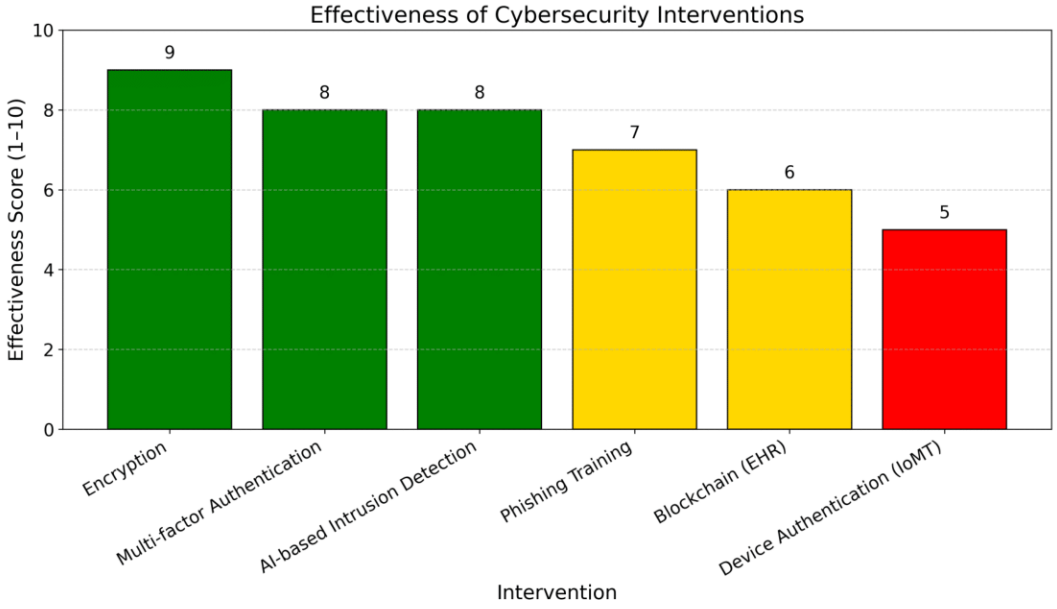

Fig. 4. Comparative effectiveness analysis of cybersecurity interventions in e-health systems, showing (from left to right) encryption, access control, intrusion detection, and staff training effectiveness scores with 95% confidence intervals.

on their frequency (x-axis) and severity of impact (y-axis). The intensity of the colors indicates the overall risk level. The map effectively displays how threats are distributed throughout the risk spectrum. Threats in the upper right

TABLE II
SUMMARY OF STUDIES ON IOT AND HEALTHCARE SECURITY

S.No	Study (Ref. No)	Approach	Key Advantages	Challenges
1	Ali et al. [4], Baral et al. [8]	IoT Device Security	Enhances eHealth security and addresses device-level vulnerabilities	LTE protocol risks; requires technical expertise
2	Andrade-Salinas et al. [5], Singh et al. [34]	Blockchain Integration	Improves healthcare data privacy and integrity via IoT-Blockchain fusion	Integration complexity; early-stage adoption
3	Archana et al. [6], Wahab et al. [37]	AI-driven Surveillance	Strengthens threat detection in cyber-physical systems	High computational cost; complex deployment
4	Coppolino et al. [13], Coppolino et al. [12], Zendehdel et al. [38]	Secure Data Auditing	Enhances integrity of wearable and clinical data	SGX configuration issues; hardware dependencies
5	Liu et al. [25], Padmaja et al. [29]	Privacy-preserving Authentication	Enables secure real-time device authentication	Latency challenges; implementation complexity
6	Awad et al. [7], Tariq et al. [35], Ksibi et al. [23]	IoT Risk Management Models	Enables adaptive, risk-aware defense strategies	Requires constant monitoring; diverse device environments

TABLE III
ORGANIZATIONAL CONSIDERATIONS IN ENHANCING CYBERSECURITY FOR E-HEALTH SYSTEMS

S.No.	Study (Ref. No)	Approach	Key Advantages	Challenges
1	Barraca et al. [9]	Incident Response Upscaling	Enhances incident response and boosts organizational cybersecurity posture	High dependency on internal support structures
2	Frontoni et al. [15]	Health Data Sharing	Enables secure exchange of patient data among general practitioners	Coordination and policy alignment challenges
3	Hatzivasilis et al. [17]	Cyber Insurance Framework	Supports continuous monitoring and coverage of cyber risks	Relies on established organizational policies
4	Hatzivasilis et al. [18]	Addressing System Vulnerabilities	Reveals internal vulnerabilities in healthcare systems	Requires proactive governance reforms
5	Sanchez-Iborra et al. [33]	Holistic Cybersecurity Architecture	Proposes an integrated platform tailored to healthcare institutions	Needs comprehensive organizational compliance
6	Venkatachalam et al. [36]	Blockchain for E-Health Records	Introduces Hyperledger-based secure record systems	Organizational inertia and adoption barriers

corner, such as interconnected medical devices (IoMT), ransomware, and insider threats, are common and severe, thus requiring urgent mitigation efforts. These threats are highlighted with the darkest colors on the map, emphasizing their priority. Moderate risk threats, such as phishing and health information exchange breaches, appear in the middle zones, underscoring the need for continuous monitoring and proactive security measures. Lower-risk issues, including vulnerabilities in telemedicine, are shown in lighter shades, indicating lower threat levels, but still worthy of attention. In general, this heat map serves as a strategic tool to prioritize cybersecurity initiatives by assessing both the likelihood and potential impact of the threat.

VI. DISCUSSION

This review draws attention to the disjointed and reactive cybersecurity posture of the global e-health ecosystem. Healthcare digitization has accelerated, but security infrastructure, policies, and awareness have not kept pace. The gaps expose healthcare systems to various threats, including vulnerabilities in IoMT devices, health information exchanges, ransomware, and insider breaches. Technical issues still dominate discourse and impact. Despite their potential, the complexity of implementation, high costs, and regulatory uncertainty prevent encryption, blockchain, and AI-based intrusion detection from being widely adopted at scale. The widespread use of cloud-based systems and networked devices without built-in security

TABLE IV
STUDIES ON LEGAL AND ETHICAL IMPLICATIONS IN HEALTHCARE SECURITY

S.No	Study (Ref. No)	Approach	Key Advantages	Challenges
1	Cellier et al. (2019) [10]	Holistic Security Method	Promotes a comprehensive perspective on healthcare cybersecurity	Navigating legal and ethical boundaries
2	Christou et al. (2020) [11]	CyberSure Framework	Improves system trust and liability handling in eHealth	Regional legal variability may hinder implementation
3	Looi et al. (2024) [26]	EHR Risk Management	Mitigates digital health record risks through proactive strategies	Requires legal and ethical alignment with practice
4	Moreno et al. (2022) [27]	ICT Integration Method	Demonstrates mHealth benefits via secure ICT integration	Exposes regulatory gaps in rapidly evolving tech environments
5	Radanliev et al. (2021) [30]	Ethical Assessment	Evaluates digital supply chain ethics in healthcare networks	Ethical considerations are often underprioritized
6	Rajamäki et al. (2022) [31]	Resilience Framework	Embeds ethical responsibility into cybersecurity planning	Legal interpretation and enforcement vary by jurisdiction

TABLE V
STUDIES ON CYBERSECURITY AWARENESS AND TRAINING

S.No.	Study (Ref. No.)	Approach	Key Advantages	Challenges
1	Aldawood et al. (2019) [3]	ICT in Cyber Security	Reviews the use of ICT tools to enhance cybersecurity posture	Limited user awareness; training program consistency
2	Giansanti et al. (2020) [16]	Risk Perception Survey	Assesses awareness levels among healthcare professionals	Difficulty in sustaining awareness over time
3	Rajamäki et al. (2023) [32]	Nurse-Focused Training	Emphasizes cybersecurity education for frontline staff	Implementation challenges in clinical environments

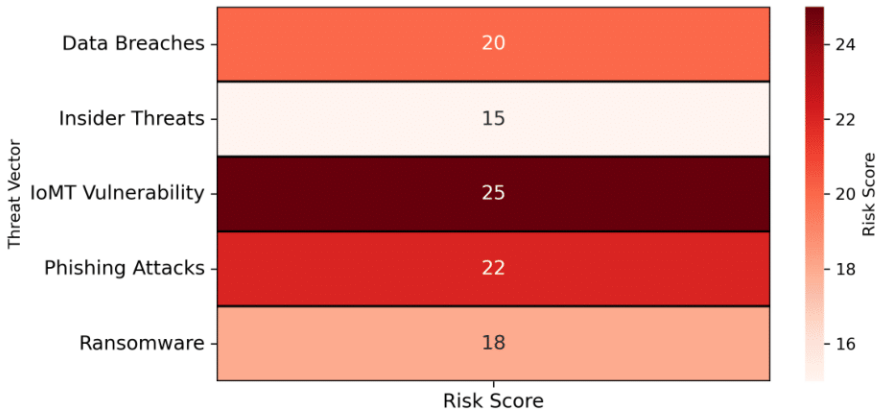

Fig. 5. Risk heat map showing threat prioritization based on frequency (x-axis) and severity (y-axis), with color intensity representing risk levels.

measures increases risk, highlighting the need for portable, healthcare-specific solutions that balance security and functionality. Organizational obstacles are just as urgent. Many healthcare organizations still lack the leadership and strategic planning necessary to manage cyber threats effectively. The lack of strong incident response procedures, frequent audits, and real-time threat monitoring fosters a reactive rather than preventative security culture. Despite being frequently cited, legal and ethical frameworks are not always applied consistently. Even though laws like GDPR and HIPAA establish crucial guidelines, there is still a gap between policy and practice. Furthermore, neither in operational contexts nor in literature do ethical principles especially those about data consent, breach transparency, and digital trust—get enough attention. Human behavior remains the most undervalued factor in e-health security. Only a small

TABLE VI
RISK ASSESSMENT OF CYBERSECURITY FACTORS IN E-HEALTH SYSTEMS

Factor	Likelihood (1–5)	Impact (1–5)	Risk Score (1–25)	Description
Malware	4	5	20	Infects systems to steal, corrupt, or disrupt data
Ransomware	4	5	20	Encrypts patient data, demands payment for decryption
Phishing	4	4	16	Deceives users to gain unauthorized access
Interconnected Devices	5	5	25	IoMT vulnerabilities allow unauthorized control or data theft
Telemedicine	3	4	12	Risks during virtual consultations and remote care
Health Info Exchanges	4	4	16	Breaches during inter-organizational data sharing
Insider Threats	4	5	20	Unauthorized access or sabotage by employees or partners

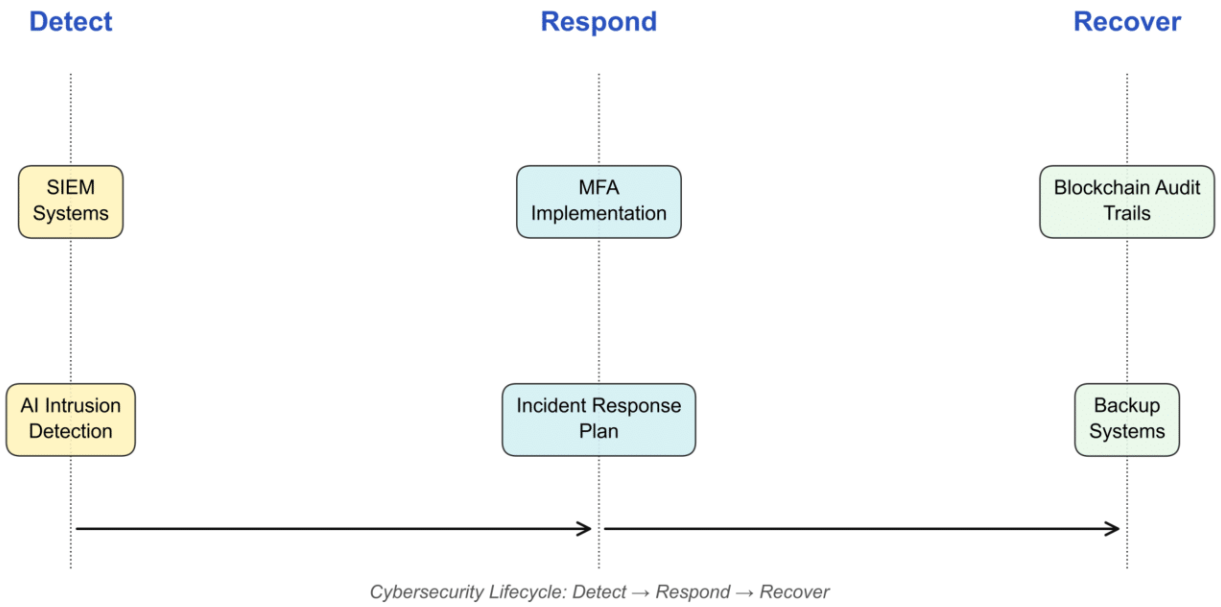

Fig. 6. Lifecycle progression of cybersecurity

percentage of the reviewed studies concentrated on structured training programs, behavioral safeguards, or cybersecurity culture-building initiatives, despite the evidence that insider threats and end-user negligence are the main causes of breaches. This imbalance limits the effectiveness of even the most sophisticated technical systems. Together, these results indicate the need for an interdisciplinary and comprehensive approach. E-health cybersecurity must be integrated into clinical workflows, governance models, compliance plans, and patient engagement procedures; it cannot be isolated within the IT department.

Figure 6 depicts the cybersecurity lifecycle in e-health systems, stressing the importance of ongoing and adaptable security measures. It outlines critical stages like risk assessment, threat mitigation, incident detection, response, and recovery. This lifecycle model shows that cybersecurity is an ongoing effort, continuously evolving to address new threats. Incorporating security at every phase—from initial design to post-incident review—helps healthcare organizations develop stronger, more proactive defense strategies.

VII. CONCLUSION

Cybersecurity can no longer be viewed as an incidental issue as healthcare systems experience a rapid digital transformation. This review emphasizes that although

there are technological solutions, organizational inertia, regulatory lag, and behavioral oversights limit their impact. In order to move toward e-health environments that are reliable and resilient, stakeholders need to take a multifaceted approach that incorporates. Strong technical protections like secure device protocols, blockchain, and AI-driven anomaly detection.Organizational changes, such as institutional accountability, ongoing monitoring, and cybersecurity leadership. Regulatory alignment, which makes sure that business procedures adhere to the goals of data protection legislation.Human-centered tactics that promote a shared responsibility and security-aware culture. The healthcare industry can only transition from reactive defenses to proactive, flexible, and patient-focused cybersecurity with the help of such an integrative framework. Strategies must change along with the threats, with cooperation, ethics, and resilience at the forefront of e-health innovation.

REFERENCES

[1] American Hospital Association, "2022 Cybersecurity Advisory," 2022. [Online]. Available: https://www.aha.org/2022-cybersecurity-advisory

[2] A. Alaqra, A. Ouda, and R. Malkawi, "Behavioral insights for cybersecurity: Exploring insider threat indicators in healthcare systems," *Computers & Security*, vol. 94, p. 101846, 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101846

[3] H. Aldawood, M. Alabadi, O. Alharbi, and G. Skinner, "A contemporary review of raising health awareness using ICT for application in the cybersecurity domain," in *Proc. Int. Conf. on Engineering Applications (ICEA)*, Article No. 8883454, 2019. [Online]. Available: https://doi.org/10.1109/CEAP.2019.8883454

[4] S. M. Ali, M. Çakmak, and Z. Albayrak, "Security classification of smart devices connected to LTE network," *Lecture Notes in Networks and Systems*, vol. 393, pp. 1125–1131, 2022. [Online]. Available: https://doi.org/10.1007/978-3-030-94191-8_91

[5] G. Andrade-Salinas, G. Salazar-Chacon, and L.-M. Vintimilla, "Integration of IoT equipment as transactional endorsing peers over a Hyperledger-Fabric blockchain network: Feasibility study," in *Communications in Computer and Information Science*, vol. 1193, pp. 95–109, 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-42517-3_8

[6] M. Archana, S. Kavitha, and A. V. Vathsala, "Auto deep learning-based automated surveillance technique to recognize the activities in the cyber-physical system," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 2, pp. 35–42, 2023. [Online]. Available: https://doi.org/10.17762/ijritcc.v11i2.6111

[7] A. I. Awad and J. Abawajy, "Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications," 2021. [Online]. Available: https://doi.org/10.1002/9781119607755

[8] S. K. Baral, R. C. Rath, R. Goel, and T. Singh, "An Application of Internet of Things for Cybersecurity and Control: Emerging Needs and Challenges," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 132, pp. 893–904, 2022. [Online]. Available: https://doi.org/10.1007/978-981-19-2347-0_69

[9] J. P. Barraca, C. Cerqueira, J. F. Alves, S. Andrade, A. Meireles, and J. R. Almeida, "Upscaling operators of essential services incident response teams," in *Proc. IEEE Symp. Comput.-Based Med. Syst. (CBMS)*, pp. 97–102, 2023. [Online]. Available: https://doi.org/10.1109/CBMS58004.2023.00199

[10] L. Cellier and S. Ghernaouti, "An interdisciplinary approach for security, privacy and trust in the electronic medical record: A pragmatic legal perspective," in *2019 IEEE International Conference on E-Health Networking, Application and Services (HealthCom)*, 2019. [Online]. Available: https://doi.org/10.1109/HealthCom46333.2019.9009588

[11] G. Christou, E. Papadogiannaki, M. Diamantaris, L. Torterolo, and P. Chatziadam, "CyberSure: A framework for liability based trust," *Lect. Notes Comput. Sci.*, vol. 11981, pp. 19–34, 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-42051-2_2

[12] L. Coppolino, S. D'Antonio, L. Romano, L. Sgaglione, and M. Staffa, "Addressing Security Issues in the eHealth Domain Relying on SIEM Solutions," in *Proc. Int. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, pp. 510–515, 2017. [Online]. Available: https://doi.org/10.1109/COMPSAC.2017.45

[13] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Facing the blockchain endpoint vulnerability: An SGX-based solution for secure eHealth auditing," *CEUR Workshop Proceedings*, vol. 2940, pp. 298–308, 2021.

[14] F. Firouzi, S. Jiang, K. Chakrabarty, B. Farahani, M. Daneshmand, J. Song, and K. Mankodiya, "Fusion of IoT, AI, Edge–Fog–Cloud, and Blockchain: Challenges, solutions, and a case study in healthcare and medicine," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 3686–3705, 2023. [Online]. Available: https://doi.org/10.1109/JIOT.2022.3191881

[15] E. Frontoni *et al.*, "Sharing health data among general practitioners: The Nu.Sa. project," *International Journal of Medical Informatics*, vol. 129, pp. 267–274, 2019. [Online]. Available: https://doi.org/10.1016/j.ijmedinf.2019.05.016

[16] D. Giansanti, M. Grigioni, L. Monoscalco, and R. A. Gulino, "A smartphone-based survey to investigate the cyber-risk perception among healthcare professionals," *IFMBE Proceedings*, vol. 76, pp. 914–923, 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-31026-4_147

[17] G. Hatzivasilis, M. Rantos, I. Askoxylakis, G. Sklavos, and C. Zidianakis, "Review of cybersecurity and privacy in healthcare systems: Technological and organizational aspects," *Sensors*, vol. 19, no. 2, p. 415, 2019. [Online]. Available: https://doi.org/10.3390/s19020415

[18] G. Hatzivasilis *et al.*, "Towards the Insurance of Healthcare Systems," in *Lecture Notes in Computer Science*, vol. 11981, pp. 185–198, 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-42051-2_13

[19] U.S. Department of Health and Human Services, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," 2022. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[20] IBM Security, "Cost of a Data Breach Report 2023," 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[21] H. S. Jennath, V. S. Anoop, and S. Asharaf, "Blockchain for healthcare: Securing patient data and enabling trusted artificial intelligence," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 3, pp. 15–23, 2020. [Online]. Available: https://doi.org/10.9781/ijimai.2020.07.002

[22] F. Jiang *et al.*, "Artificial Intelligence in Healthcare: Past, Present and Future," *Stroke and Vascular Neurology*, vol. 6, no. 3, pp. 230–243, 2021. [Online]. Available: https://doi.org/10.1136/svn-2020-000448

[23] S. Ksibi, F. Jaidi, and A. Bouhoula, "A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach," *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 107–127, 2023. [Online]. Available: https://doi.org/10.1007/s11036-021-01799-6

[24] X. Li, J. Jiang, L. Wang, and W. He, "Enhancing healthcare security awareness through training and policy implementation," *BMC Health Services Research*, vol. 19, p. 255, 2019. [Online]. Available: https://doi.org/10.1186/s12913-019-4081-4

[25] X. Liu, W. Ma, and H. Cao, "MBPA: A Medibchain-based privacy-preserving mutual authentication in TMIS for mobile medical cloud architecture," *IEEE Access*, vol. 7, pp. 149282–149298, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2947313

[26] J. C. L. Looi, S. Allison, T. Bastiampillai, P. A. Maguire, S. Kisely, and R. C. H. Looi, "Mitigating the consequences of electronic health record data breaches for patients and healthcare workers," *Australian Health Review*, vol. 48, no. 1, pp. 4–7, 2024. [Online]. Available: https://doi.org/10.1071/AH23258

[27] I. M. Moreno and M. N. M. Vida, "E-health. Towards 5P medicine: personalized, precise, preventive, predictive and participatory medicine," *Revista de Derecho de la Seguridad Social, Laborum*, no. 4, pp. 415–443, 2022.

[28] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 2022. [Online]. Available: https://www.nist.gov/cyberframework

[29] K. Padmaja and R. Seshadri, "A real-time secure medical device authentication for personal E-Healthcare services on cloud computing," *Int. J. Syst. Assur. Eng. Manag.*, 2021. [Online]. Available: https://doi.org/10.1007/s13198-021-01148-1

[30] P. Radanliev, D. De Roure, U. Ani, and G. Carvalho, "The ethics of shared COVID-19 risks: An epistemological framework for ethical health technology assessment of risk in vaccine supply chain infrastructures," *Health Technol.*, vol. 11, no. 5, pp. 1083–1091, 2021. [Online]. Available: https://doi.org/10.1007/s12553-021-00565-3

[31] J. Rajamäki and A. Hummelholm, "Ethical resilience management framework for critical healthcare information infrastructure," *WSEAS Transactions on Biology and Biomedicine*, vol. 19, pp. 67–76, 2022. [Online]. Available: https://doi.org/10.37394/23208.2022.19.9

[32] RajamäkDevi, N. G. S., and Singh, N. S. (2023). *ECT-ABE Algorithm-Based Secure Preserving Framework for Medical Big Data*. Lecture Notes in Networks and Systems, **587**, 841–850. doi:10.1007/978-981-19-7874-6_61.

[33] R. Sanchez-Iborra and A. Skarmeta, "Securing the hyperconnected healthcare ecosystem," *Lect. Notes Data Eng. Commun. Technol.*, vol. 105, pp. 455–471, 2022. [Online]. Available: https://doi.org/10.1007/978-3-030-90618-4_22

[34] P. K. Singh, "Next Generation Wireless Communication: Facilitated by Machine Learning," *Lecture Notes in Electrical Engineering*, vol.

855, pp. 779–793, 2022. [Online]. Available: https://doi.org/10.1007/978-981-16-8892-8_59

[35] N. Tariq, F. A. Khan, and M. Asim, "Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis," *Procedia Comput. Sci.*, vol. 191, pp. 425–430, 2021. [Online]. Available: https://doi.org/10.1016/j.procs.2021.07.055

[36] N. Venkatachalam, P. O'Connor, and S. Palekar, "Cyber security and cyber resilience for the Australian e-health records: A blockchain solution," in *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*, pp. 799–816, 2022. [Online]. Available: https://doi.org/10.4018/978-1-6684-7132-6.ch044

[37] F. Wahab *et al.*, "An AI-driven hybrid framework for intrusion detection in IoT-enabled e-health," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 6096289, 2022. [Online]. Available: https://doi.org/10.1155/2022/6096289

[38] G. A. Zendehdel, R. Kaur, I. Chopra, N. Stakhanova, and E. Scheme, "Automated Security Assessment Framework for Wearable BLE-enabled Health Monitoring Devices," *ACM Trans. Internet Technol.*, vol. 22, no. 1, article 3448649, 2022. [Online]. Available: https://doi.org/10.1145/3448649

Dr. Jyoti Badge was born in 1979 in Bhopal, Madhya Pradesh. She completed her graduation in Mathematics from Govt. M.L.B. Girls P.G. College, Bhopal, in 2000, followed by a master's degree in Statistics from Govt. Motilal Vigyan Mahavidyalaya, Bhopal, in 2003. She earned her Ph.D. in Applied Mathematics from Maulana Azad National Institute of Technology (MANIT), Bhopal, in 2012. Currently, she serves as an Assistant Professor at VIT University, Bhopal, with over 15 years of teaching experience in Statistics. Her research and teaching interests include Business Mathematics, Business Statistics, Quantitative Techniques, and Econometrics for Finance.