

Navigating cybersecurity paradox: opportunities and risks of artificial intelligence integration in healthcare systems

Rani Tiyas Budiyanthi¹, Roro Isyawati Permata Ganggi²

¹Department of Health Policy and Administration, Faculty of Public Health, Universitas Diponegoro, Semarang, Indonesia

²Library and Information Science Study Program, Faculty of Humanities, Universitas Diponegoro, Semarang, Indonesia

Article Info

Article history:

Received Aug 26, 2025

Revised Aug 3, 2026

Accepted Aug 12, 2026

Keywords:

Artificial intelligence
Cybersecurity risk and protection
Healthcare security
Paradoxical function of AI
Patient data privacy
Trust and safety in digital health

ABSTRACT

Artificial intelligence (AI) has been widely used in healthcare services, such as assisting in diagnosis and clinical decision-making. AI can potentially improve cybersecurity within healthcare services. Nevertheless, AI can also pose new threats that are dangerous to the system. The objective of this research is to investigate the contradictory roles that AI plays in the context of healthcare security. This study was a bibliometric study and systematic review from the Scopus database that were published in 2015-2025. This research shows that AI can bring benefits for security, such as enhanced threat detection, automation, and efficiency, as well as improved patient care. However, AI has many risks and challenges in healthcare security, such as new vulnerabilities, data privacy concerns, and ethical and bias issues. Integration of AI in healthcare services, especially to strengthen cybersecurity, needs to be accompanied by clear regulations, robust data protection standards, and ongoing supervision. In addition, principles of patient data security and privacy must be carefully observed to balance the benefits of using AI in healthcare security with the potential risks that may arise.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Rani Tiyas Budiyanthi

Department of Health Policy and Administration, Faculty of Public Health, Universitas Diponegoro

Semarang, Indonesia

Email: ranitiyas@lecturer.undip.ac.id

1. INTRODUCTION

The rapid advancement of digital technology in recent decades has significantly transformed the healthcare industry, such as the use of electronic medical records, electronic health records, telemedicine services, and artificial intelligence (AI) [1], [2]. These digital platforms have revolutionized the collection, storage, and utilization of patient data, allowing healthcare providers to efficiently access comprehensive patient information [3]–[5]. The substantial volume of data generated by these systems has introduced the concept of "big data" in healthcare, which can be harnessed to support evidence-based decision-making, enhance patient outcomes, and improve overall healthcare delivery [6], [7].

AI has emerged as a potent tool capable of analyzing complex datasets to provide insights and support clinical decision-making processes [8], [9]. As patient data becomes increasingly digitized and interconnected, the risk of data breaches and unauthorized access escalates exponentially. Incidents involving data breaches and leaks within healthcare facilities have persistently risen in recent years, encompassing theft of personal information, manipulation of medical data, and even threats to patient safety, such as cyberterrorism [10]. The healthcare sector is an appealing target for cybercriminals because of two primary factors: the abundance of valuable data and its relatively weak defenses. This situation poses potential harm to patients as it may result in data leakage, disruption, or inaccessibility [11], [12]. On the other hand, AI has fundamentally transformed the field of cybersecurity by introducing advanced capabilities

in threat detection and prevention [13], [14]. On the other hand, AI can also pose new threats that are dangerous to the system [15], [16].

Although there have been many papers discussing AI and cybersecurity, there has not yet been a paper that specifically addresses the paradoxical function of AI in cybersecurity within healthcare services. This is particularly from the perspective of benefits and challenges as well as strategies to overcome them. This research aims to explore the threat and shield function of AI in healthcare in the context of healthcare security, and the strategy to implement AI in healthcare cybersecurity.

2. METHOD

2.1. Data search

In the Scopus database, a search was performed to find articles discussing both the advantages and difficulties of implementing AI in cybersecurity within healthcare services. The search utilized the keywords "artificial intelligence" OR "AI" AND "cybersecurity" AND "healthcare". The use of the Scopus database was intended because this database is multidisciplinary, thus covering the aspects of healthcare services, security, and information systems.

2.2. Inclusion and exclusion criteria

Articles discussing the advantages and obstacles of using AI in healthcare services, published between 2015 and 2025, are part of the inclusion criteria for this study. The exclusion criteria are articles that are not in English, review articles, and are not relevant to the topic under study. The selection of inclusion and exclusion criteria is intended to ensure that the results of the study align with the objectives to be achieved.

2.3. Quantitative (bibliometric analysis)

Bibliometric analysis using biblioshiny was conducted to observe trend analysis, productive countries, co-occurrence networks analysis, and thematic analysis. Trend analysis aims to determine the increase in the number of publications from year to year in accordance with the topic under study. Analysis related to productive countries aims to identify countries with research concerns regarding AI and cybersecurity in health care. Meanwhile, co-occurrence network and thematic map analyses aim to identify currently developing research areas or topics and topics that may be further explored in subsequent research. The descriptive analysis of the gathered data involved a comprehensive examination of overall patterns, trends, and relationships within the dataset.

2.4. Data mapping

After obtaining data related to publications relevant to the topic under study, mapping of articles relevant to the benefits and challenges in the use of AI for digital health service security was carried out. The data extraction process involved creating a comprehensive table to organize information from the selected studies systematically related to publications concerning the benefits and risks of AI in healthcare security. This table included columns for the authors' names and publication years, providing a clear chronological overview of the research.

2.5. Data analysis and reporting

This process entailed systematically categorizing and summarizing the information to provide a clear overview of the current state of knowledge related to the paradoxical function of AI in healthcare security systems. The results obtained are then synthesized and presented in the form of a descriptive narrative. Through the combination of bibliometric analysis and systematic review conducted, research gaps can be identified, the benefits and challenges in the implementation of AI in digital health service security can be further analyzed, and insights for future research can be recommended.

3. RESULTS AND DISCUSSION

3.1. Trend publication

The exponential growth in publications related to AI and cybersecurity in healthcare since 2018 underscores the increasing importance and relevance of these interconnected fields. This surge in research output reflects the rapid technological advancements in AI and the growing awareness of cybersecurity threats in the healthcare sector. As healthcare systems become more digitized and interconnected, the need for robust AI-driven security measures has become paramount, driving researchers and practitioners to explore innovative solutions to protect sensitive patient data and critical healthcare infrastructure.

The projected publication count of 523 documents from 2018 until 2025 indicates a sustained and intensifying focus on this interdisciplinary area. This trend suggests that the healthcare industry is actively seeking to leverage AI technologies to enhance cybersecurity measures, improve threat detection, and develop more resilient systems. The annual increase in publications, particularly over the last decade, demonstrates the evolving nature of both AI capabilities and cybersecurity challenges in healthcare, as shown in Figure 1. This continuous growth in research output not only highlights the urgency of addressing cybersecurity concerns but also points to the potential for AI to revolutionize healthcare security practices, ultimately contributing to safer and more efficient healthcare delivery systems. This shows a great opportunity and potential for utilizing AI to enhance security in healthcare [17].

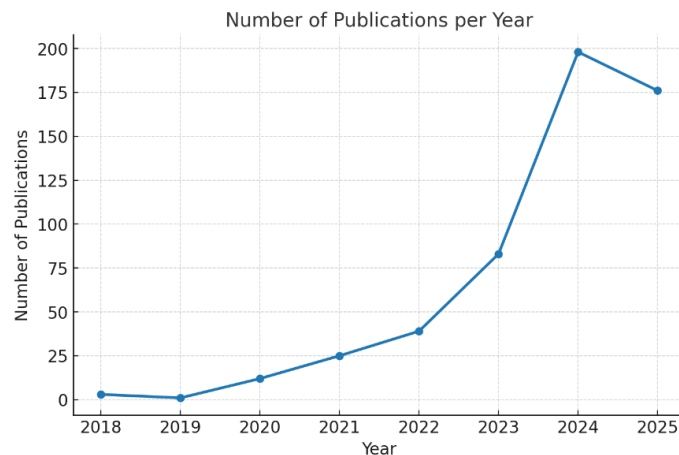


Figure 1. Trend publication related to cybersecurity and AI in healthcare

The distribution of publications related to AI and cybersecurity in healthcare reveals a significant global interest in these interconnected fields, as shown in Figure 2. India emerges as the leading contributor with 179 documents, showcasing its strong focus on AI technologies and healthcare security. The United States follows closely with 110 documents, reflecting its advanced research infrastructure and technological capabilities. Saudi Arabia's third-place ranking with 44 documents indicates a growing emphasis on healthcare innovation in the Middle East.

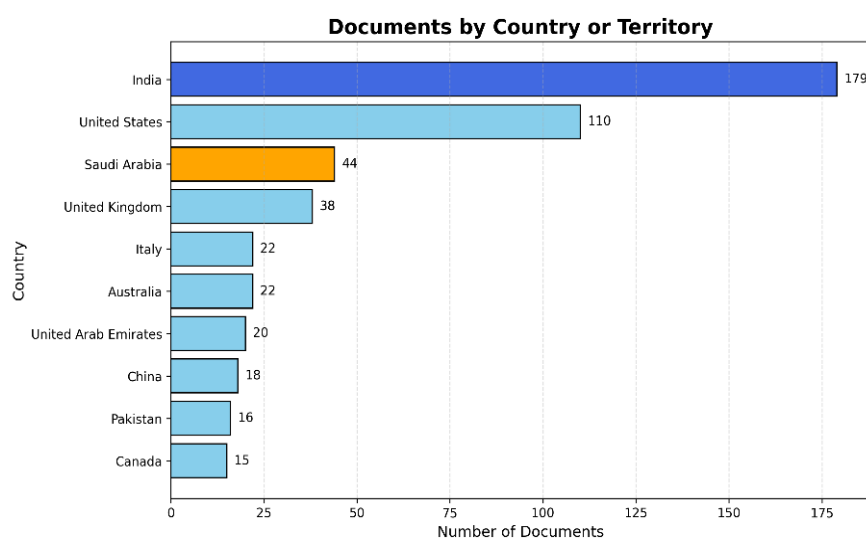


Figure 2. The number documents by the country or territory related to AI and cybersecurity in healthcare

The presence of diverse countries in the top ten list, including European nations like the United Kingdom and Italy, as well as Australia and Canada, underscores the worldwide recognition of the importance of AI and cybersecurity in healthcare. China's inclusion, albeit with fewer documents, suggests its increasing involvement in this research area. The representation of developing nations such as Pakistan and the United Arab Emirates highlights the global nature of these technological advancements and the potential for collaborative efforts to address healthcare challenges through AI and enhanced cybersecurity measures. This indicates that the trend of cybersecurity in the use of AI in healthcare services is a global issue in various countries. The Department of Health, Disability, and Ageing Australia has even published the safe and responsible AI in health care legislation and regulation review to reexamine the standards for safe utilization of AI in the health sector [18].

The predominance of conference papers and articles in the field of cybersecurity and AI in healthcare, as indicated by the Scopus databases, suggests a rapidly evolving and dynamic research landscape. Conference papers often represent cutting-edge research and preliminary findings, allowing for quick dissemination of new ideas and technologies. This format is particularly suitable for the fast-paced nature of both cybersecurity and AI, where innovations can occur rapidly. Articles, on the other hand, typically offer more in-depth analyses and comprehensive studies, providing a solid foundation for the field's knowledge base.

The nearly equal distribution between conference papers (128 documents) and articles (127 documents) indicates a balanced approach to knowledge sharing in this domain. This balance suggests that researchers are actively presenting their work at conferences for immediate feedback and discussion, while also dedicating time to more thorough investigations suitable for journal publications. Such a distribution is beneficial for the field, as it combines the immediacy of conference presentations with the rigor of peer-reviewed articles, fostering both rapid innovation and thorough scientific scrutiny in the intersection of cybersecurity, AI, and healthcare.

3.2. Co-occurrence network analysis

Based on co-occurrence network analysis as in Figure 3, the data showed that there are three dominant clusters. The red cluster represents the application of AI in healthcare services, focusing on improving healthcare services such as disease diagnosis using AI, smart hospitals, IoT in healthcare services, clinical decision support, predictive analysis, and medical imaging. The blue cluster discusses cybersecurity and information security, focusing on research related to cybersecurity in health information systems, especially regarding patient data protection, cyber-attack detection, ransomware in hospitals, intrusion detection, blockchain security, and AI-based threat detection. This topic is the most frequently discussed theme, indicating growing attention to cyber threats in healthcare services. The green cluster relates to supporting technologies or data analytics, which is relatively smaller compared to the other two clusters. This topic serves as a supporting theme for research in AI and cybersecurity, particularly concerning data mining, optimization, feature selection, data analysis, and computational intelligence. An interesting finding is the presence of many gray lines connecting the red and blue clusters, indicating that AI is not only used to improve healthcare services but is also utilized in cybersecurity within healthcare services. The most dominant keywords in several of these clusters are listed in Table 1.

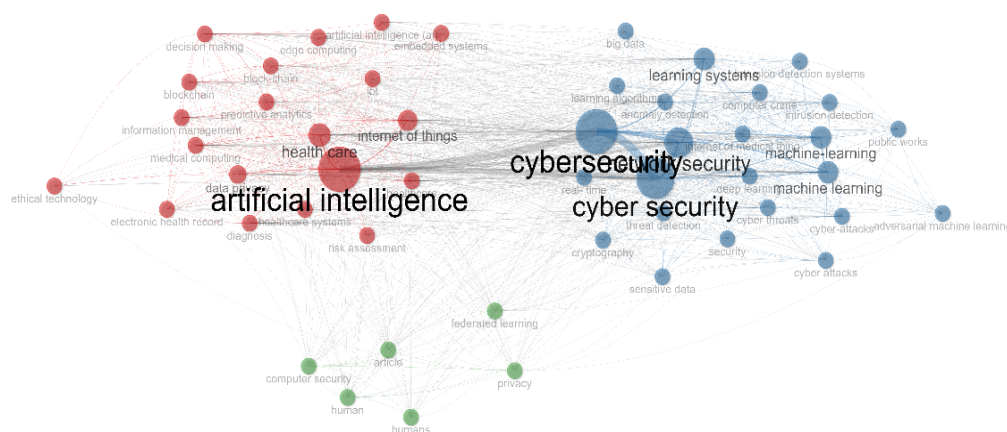


Figure 3. Co-occurrence network analysis related to AI and cybersecurity in healthcare services

Table 1. Dominant keywords in the three clusters

Keyword	Interpretation
Cybersecurity	The main focus of research on health system safety
Artificial intelligence	The main technologies that are widely used or applied
Healthcare	Main areas of AI application
Internet of things	AI system supporter

This map shows that current research has shifted from AI for healthcare services toward integration with cybersecurity in healthcare services. Issues such as patient data protection, AI-based cyber threats, security of medical IoT devices, and the development of safe AI have become the main focus of research. This issue has continued to develop, especially in the post-COVID-19 pandemic period, during which healthcare services have been extensively developed and implemented digitally to expand the reach of healthcare delivery [19].

3.3. Thematic map analysis

In the thematic analysis based on niche themes, motor themes, emerging themes, and basic themes, the results are presented in Figure 4. Motor themes have high centrality and high density, with health care, data privacy, and medical computing as the most developed and influential themes in the overall research topics. Data privacy and patient data protection are increasingly discussed topics in the digitalization of health care services.

In niche themes with high density and low centrality, several themes such as machine learning and deep learning were identified. This indicates that these themes are developing rapidly, but their relevance to cybersecurity in healthcare services is still limited. In basic themes, high centrality and low density were observed with themes related to internet of things, decision making, and blockchain. This suggests future research directions that may combine AI, IoT, and cybersecurity in healthcare.

Meanwhile, in the emerging theme, the topics of AI and cybersecurity appear with low density and relatively low centrality. This indicates that these two topics are new and currently developing themes. Based on the thematic map, several research opportunities remain open, including the integration of AI with blockchain to enhance the security of electronic medical records, the application of AI in detecting cyberattacks on healthcare IoT devices, AI-based patient data privacy governance models in accordance with data protection regulations, security frameworks for telemedicine that combine AI, blockchain, and IoT, as well as the use of machine learning for cyber threat detection in electronic medical records.

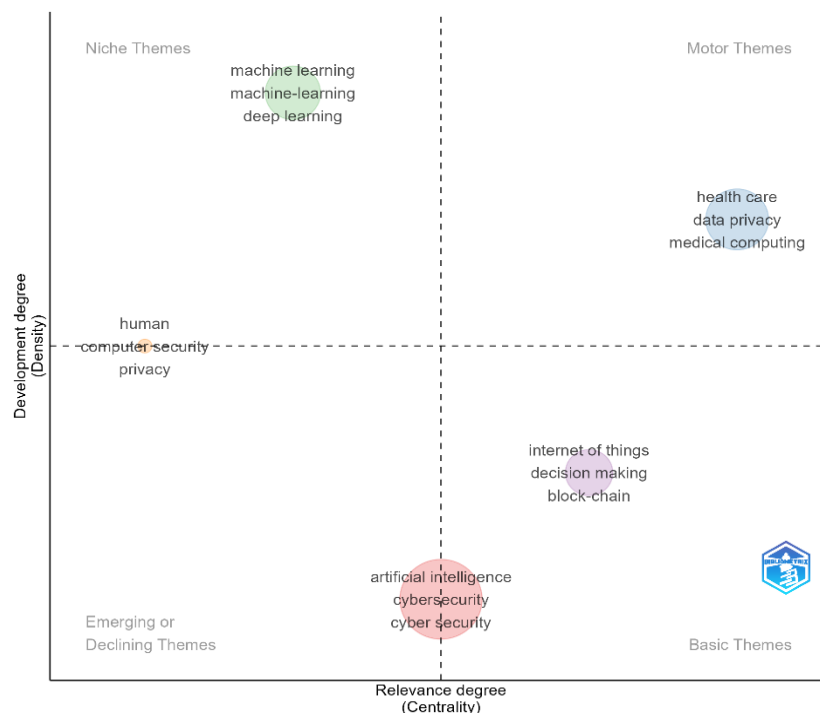


Figure 4. Thematic map analysis related to AI and cybersecurity in healthcare

3.4. Paradoxical function of AI in healthcare cybersecurity

Based on existing publications, a review and further analysis were conducted of related literature on the paradoxical functions of AI in cybersecurity in healthcare services, and several articles were identified as listed in Table 2. The results indicate that studies on the use of AI in digital healthcare security began to develop in 2023. In addition to exploring the benefits, research on the potential and impacts arising has also progressed.

Table 2. Articles related to AI and security in healthcare

No	Author	Year	Main result
1	Musa and Abdulfatai [20]	2024	Leveraging AI to improve cybersecurity in healthcare systems and the challenges of that implementation.
2	Shukla [21]	2025	The role of AI in enhancing cybersecurity in healthcare includes anomaly detection, predictive analytics, and the recommendation of anticipated and mitigated threats. This paper also discusses the standards, guidelines, and legal framework related to the implementation of AI for improving cybersecurity in healthcare.
3	Kuznetsov <i>et al.</i> [22]	2024	AI-driven platforms are designed to adapt and evolve in response to cyber threats, predicting future vulnerabilities. AI technologies, such as machine learning algorithms, can detect and process natural language for advanced predictive analytics.
4	Tyagi <i>et al.</i> [23]	2023	AI's utilization to improve cybersecurity in Digital Health Communication (DHC) and protect patient privacy
5	Kioskli <i>et al.</i> [24]	2025	The framework for assessing risk and conformity, along with the certification scheme, was examined to oversee the application of AI in practices such as risk management, security evaluations, risk forecasting, security measures, and ongoing monitoring.
6	Ndumbe and Velikov [25]	2024	The strategies of healthcare cybersecurity implementation in the United Kingdom and explore the impact of AI's implementation on cybersecurity and healthcare.
7	Gupta <i>et al.</i> [26]	2025	The contribution of AI to strengthening healthcare security and boosting patient outcomes.
8	Amutha <i>et al.</i> [27]	2025	AI implementation can enhance security, but also discusses the risk of AI in healthcare security.
9	Monteith <i>et al.</i> [28]	2024	The types of AI that can be a threat to individuals and the healthcare sector, and potential ways to mitigate risks, including the use of AI predictive tools.
10	Bonagiri <i>et al.</i> [29]	2024	The impact of AI-driven technology on the healthcare industry is especially focused on patient data and medical device protection.
11	Kshetri and Voas [30]	2025	Process and procedure of agentic AI to enhance cybersecurity.
12	Saadallah <i>et al.</i> [31]	2025	A framework for integration of AI, automation, and human expertise to ensure security, accessibility, and adaptability.
13	Jain <i>et al.</i> [32]	2024	Propose a cybersecurity framework standard, such as the NIST cybersecurity framework or ISO 27001.

The use of AI in cybersecurity for healthcare services presents a paradoxical situation. On one hand, AI can enhance cybersecurity; however, on the other hand, the use of AI also introduces new threats. Machine learning algorithms and predictive analytics, which are forms of AI, enhance the capacity to identify and address cyber threats as they occur in real-time. Machine learning algorithms can continuously analyze large amounts of data, system logs, and user behavior patterns to establish patterns and quickly identify anomalies that indicate security threats [33]. These AI-powered systems can detect subtle deviations from typical patterns that human analysts might overlook, enabling faster and more accurate threat detection [33].

Predictive analytics, another key AI application, can anticipate potential vulnerabilities and attack vectors before they are exploited [34], [35]. By analyzing historical data on past breaches, current threat intelligence, and emerging cybersecurity trends, these systems can forecast likely areas of risk and prioritize security measures accordingly. This proactive approach allows healthcare organizations to allocate resources more effectively, strengthening defenses in critical areas before attacks occur. Additionally, AI-driven automation can streamline incident response processes, reducing the time between threat detection and mitigation, thus minimizing potential damage and data loss in the event of a breach [20]–[22].

AI can also respond to an incident or cyberattack automatically and control its implementation. This reduces the time and effort required [23]. It also helps healthcare anticipate and mitigate threats more effectively. The proactive nature of AI in cybersecurity extends beyond immediate incident response [36], [37]. By analyzing vast amounts of data from various sources, including network traffic, user behavior, and global threat intelligence feeds, AI can predict potential vulnerabilities and emerging attack vectors. This predictive capability allows healthcare organizations to implement preemptive measures, such as patching systems, updating security protocols, or reinforcing access controls, before a threat materializes [21], [22], [38]. By

improving the healthcare security system, AI ensures the integrity and safety of patient data, that was crucial for accurate diagnosis, personalized medicine, and overall patient care [24], [25], [27]. Although AI can improve healthcare security, on the other hand, integrating AI in the healthcare system will introduce new cybersecurity challenges. AI systems themselves can be targeted by cyber or adversarial attacks when malware manipulates the AI algorithm to bypass security, which can lead to system failures [28]. The complexity of AI systems in healthcare also increases the attack surface. As these systems become more interconnected and rely on vast amounts of data, they present more entry points for cybercriminals. Moreover, the black-box nature of some AI algorithms makes it challenging to detect and understand when a system has been compromised [39], [40]. Healthcare organizations must therefore implement robust security protocols specifically designed for AI systems, including regular audits, adversarial testing, and continuous monitoring. Balancing the benefits of AI in healthcare with the need for stringent cybersecurity measures remains a critical challenge for the industry [29], [30], [41].

AI's reliance of AI on large datasets also raises significant concerns related to patient data privacy. Ensuring an AI system with regulations and ethical guidelines is needed to maintain transparency and protect sensitive health data and information [31], [42], [43]. To address these concerns, healthcare organizations and AI developers must prioritize transparency in their data handling practices and AI algorithms [44]. This includes clearly communicating to patients how their data will be used, obtaining informed consent, and providing options for individuals to share their data [45], [46]. Additionally, implementing stringent data anonymization techniques, encryption protocols, and access controls can help mitigate the risk of data breaches and unauthorized disclosures. Regular audits and compliance checks should be conducted to ensure adherence to established regulations and ethical standards, fostering trust between patients, healthcare providers, and AI systems [22], [24], [28]. AI-driven cybersecurity can also lead to ethical issues related to potential biases in its algorithms. This can affect the accuracy and fairness of responses and threat detection [22], [28], [32].

To navigate this paradoxical function of AI in healthcare cybersecurity, healthcare organizations must adopt many strategies or approaches. First, a comprehensive cybersecurity framework is required, such as the NIST Cybersecurity Framework or ISO 27001. It can help manage risks and ensure compliance with regulatory standards [32]. Second, continuous monitoring and adaptation should be regularly performed. AI standards should be assessed before and during implementation. AI should be designed to continuously learn and adapt to evolving threats and ensure that it remains effective against new attack patterns [22], [47], [48]. This implementation necessitates a multidisciplinary approach, bringing together healthcare providers, cybersecurity specialists, and regulatory bodies to ensure the responsible and ethical application of AI in healthcare [25].

Healthcare providers can contribute their clinical expertise and understanding of patient needs, while cybersecurity experts address potential vulnerabilities and safeguard sensitive medical data [17], [49]. Regulatory bodies play a crucial role in establishing and enforcing guidelines that balance innovation with patient safety and privacy concerns [50], [51]. By fostering open communication and knowledge sharing among these diverse stakeholders, the healthcare industry can harness the benefits of AI technology while maintaining the highest standards of patient care, data protection, and ethical practice.

4. CONCLUSION

The use of AI in cybersecurity within healthcare services has become a focus and concern of research in recent years, particularly regarding privacy, data security, and patient protection in healthcare services. AI has the potential to significantly enhance cybersecurity in healthcare by improving threat detection, automation, and operational efficiency while also advancing patient care. However, the integration of AI into healthcare security is accompanied by numerous risks and challenges, including the emergence of new vulnerabilities, concerns regarding data privacy, and issues related to ethics and bias. To effectively address these challenges, strategies such as AI standardization, continuous monitoring and adaptation, and collaboration across multiple sectors are essential for the successful implementation of AI in healthcare cybersecurity contexts.

ACKNOWLEDGMENTS

The authors would like to thank Universitas Diponegoro for supporting this research implementation.

FUNDING INFORMATION

The funding for this research was provided by Universitas Diponegoro under the research article review (RAR) 2025, with the contract number 222-029.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rani Tiya Budiyan	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Roro Isyawati Permata		✓	✓			✓		✓	✓	✓			✓	
Ganggi														

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

INFORMED CONSENT

This research did not include any individuals or personal identification details that would necessitate obtaining informed consent.

ETHICAL APPROVAL

This study does not involve any human or animal subjects, and no research was conducted with human participants. Consequently, the authors did not seek approval from an institutional review board.

DATA AVAILABILITY

This paper does not include a data availability section because no new data were generated or examined in this study.

REFERENCES

- [1] M. Hossian, "Electronic medical record and electronic health record have potential to improve quality of care," *Academia Letters*, vol. 2, Jul. 2021, doi: 10.20935/AL1565.
- [2] M. Ibrahim, M. A. Mahmoud, M. A. Al-Sharafi, and A. Hassan, "A decade-long bibliometric analysis of electronic health record research trends (2014–2024)," in *Current and Future Trends on AI Applications*, Cham, Switzerland: Springer, 2025, pp. 37–53, doi: 10.1007/978-3-031-75091-5_3.
- [3] V. Ehrenstein, H. Kharrazi, H. Lehmann, and C. O. Taylor, "Obtaining data from electronic health records," in *Registries for Evaluating Patient Outcomes: A User's Guide*, Rockville, Maryland: AHRQ Publication, 2019, pp. 52–74.
- [4] R. Canaway *et al.*, "Gathering data for decisions: best practice use of primary care electronic records for research," *Medical Journal of Australia*, vol. 210, no. S6, Apr. 2019, doi: 10.5694/mja2.50026.
- [5] B. B. Dean, J. Lam, J. L. Natoli, Q. Butler, D. Aguilar, and R. J. Nordyke, "Use of electronic medical records for health outcomes research: a literature review," *Medical Care Research and Review*, vol. 66, no. 6, pp. 611–638, Dec. 2009, doi: 10.1177/1077558709332440.
- [6] S. G. Peters and J. D. Buntrock, "Big data and the electronic health record," *Journal of Ambulatory Care Management*, vol. 37, no. 3, pp. 206–210, Jul. 2014, doi: 10.1097/JAC.000000000000037.
- [7] H. Hemingway *et al.*, "Big data from electronic health records for early and late translational cardiovascular research: challenges and potential," *European Heart Journal*, vol. 39, no. 16, pp. 1481–1495, Apr. 2018, doi: 10.1093/eurheartj/ehx487.
- [8] C. Giordano, M. Brennan, B. Mohamed, P. Rashidi, F. Modave, and P. Tighe, "Accessing artificial intelligence for clinical decision-making," *Frontiers in Digital Health*, vol. 3, Jun. 2021, doi: 10.3389/fdgth.2021.645232.
- [9] F. Magrabi *et al.*, "Artificial intelligence in clinical decision support: challenges for evaluating AI and practical implications," *Yearbook of Medical Informatics*, vol. 28, no. 1, pp. 128–134, Aug. 2019, doi: 10.1055/s-0039-1677903.
- [10] S. Rai, R. Sharma, D. Mishra, and N. Pathak, "Cyber terrorism in health information systems: a systematic review and bibliometric analysis," in *Intersections of Law and Computational Intelligence in Health Governance*, Hershey, Pennsylvania: IGI Global Scientific Publishing, 2024, pp. 220–247, doi: 10.4018/979-8-3693-5976-1.ch011.
- [11] P. Ewoh and T. Vartiainen, "Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review," *Journal of Medical Internet Research*, vol. 26, May 2024, doi: 10.2196/46904.
- [12] A. Sardi, A. Rizzi, E. Sorano, and A. Guerrieri, "Cyber risk in health facilities: a systematic literature review," *Sustainability*, vol. 12, no. 17, Aug. 2020, doi: 10.3390/su12177002.

- [13] S. Arefin and M. Simcox, "AI-driven solutions for safeguarding healthcare data: innovations in cybersecurity," *International Business Research*, vol. 17, no. 6, Nov. 2024, doi: 10.5539/ibr.v17n6p74.
- [14] M. Rizvi, "Enhancing cybersecurity: the power of artificial intelligence in threat detection and prevention," *International Journal of Advanced Engineering Research and Science*, vol. 10, no. 5, pp. 55–60, 2023, doi: 10.22161/ijaers.105.8.
- [15] N. N. Botha *et al.*, "Artificial intelligence in healthcare: a scoping review of perceived threats to patient rights and safety," *Archives of Public Health*, vol. 82, no. 1, Oct. 2024, doi: 10.1186/s13690-024-01414-1.
- [16] F. Federspiel, R. Mitchell, A. Asokan, C. Umana, and D. McCoy, "Threats by artificial intelligence to human health and human existence," *BMJ Global Health*, vol. 8, no. 5, May 2023, doi: 10.1136/bmjgh-2022-010435.
- [17] M. U. Tariq, "Enhancing cybersecurity protocols in modern healthcare systems: strategies and best practices," in *Transformative Approaches to Patient Literacy and Healthcare Innovation*, Hershey, Pennsylvania: IGI Global Scientific Publishing, 2024, pp. 223–241, doi: 10.4018/979-8-3693-3661-8.ch011.
- [18] Australian Government, "Safe and responsible artificial intelligence in health care – legislation and regulation review," health.gov.au, 2025. Accessed: July 31, 2025. [Online]. Available: <https://www.health.gov.au/resources/publications/safe-and-responsible-artificial-intelligence-in-health-care-legislation-and-regulation-review-final-report?language=en>
- [19] R. Abdolkhani, S. Petersen, R. Walter, L. Zhao, K. B.-Henderson, and K. Livesay, "The impact of digital health transformation driven by COVID-19 on nursing practice: systematic literature review," *JMIR Nursing*, vol. 5, no. 1, Aug. 2022, doi: 10.2196/40348.
- [20] A. Musa and A. O. Abdulfatai, "Artificial intelligence for secured cybersecurity in emerging healthcare systems," in *Cybersecurity in Emerging Healthcare Systems*, United Kingdom: The Institution of Engineering and Technology, 2024, pp. 203–240, doi: 10.1049/PBHE064E_ch7.
- [21] A. Shukla, "AI for healthcare security: the intersection of innovation and resilience," in *Secure and Resilient Digital Transformation of Healthcare (SUNRISE 2024)*, Cham, Switzerland: Springer, 2025, pp. 109–127, doi: 10.1007/978-3-031-85558-0_6.
- [22] O. Kuznetsov, E. Frontoni, N. Kryvinska, D. P.-Tkachenko, and B. Khruskov, "Adaptive cybersecurity: AI-driven threat intelligence in healthcare systems," in *Cybersecurity in Emerging Healthcare Systems*, United Kingdom: The Institution of Engineering and Technology, 2024, pp. 75–106, doi: 10.1049/PBHE064E_ch3.
- [23] A. K. Tyagi, V. Hemamalini, and G. Soni, "Digital health communication with artificial intelligence-based cyber security," in *AI-Based Digital Health Communication for Securing Assistive Systems*, Hershey, Pennsylvania: IGI Global Scientific Publishing, 2023, pp. 178–213, doi: 10.4018/978-1-6684-8938-3.ch009.
- [24] K. Kioskli, E. Grigoriou, S. Islam, A. M. Yiorkas, L. Christofi, and H. Mouratidis, "A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain," *International Journal of Information Security*, vol. 24, no. 2, Apr. 2025, doi: 10.1007/s10207-025-01009-z.
- [25] S. I. Ndumbe and P. Velikov, "Government strategies on cybersecurity and how artificial intelligence can impact cybersecurity in healthcare with special reference to the UK," in *Cybersecurity and Artificial Intelligence*, Cham, Switzerland: Springer, 2024, pp. 217–236, doi: 10.1007/978-3-031-52272-7_9.
- [26] S. Gupta, M. Kapoor, and S. K. Debnath, *Artificial intelligence-enabled security for healthcare systems: safeguarding patient data and improving services*. Cham, Switzerland: Springer, 2025, doi: 10.1007/978-3-031-82810-2.
- [27] S. Amutha, G. U. Maheswari, G. Nallasivan, M. S. Nisha, K. Ramanan, and A. A. Lakshmi, "Enhancing security for smart healthcare systems and infrastructure with artificial intelligence," in *Cybersecurity and Data Science Innovations for Sustainable Development of HEICC*, Boca Raton, Florida: CRC Press, 2025, pp. 108–122.
- [28] S. Monteith, T. Glenn, J. R. Geddes, E. D. Achtyes, P. C. Whybrow, and M. Bauer, "Artificial intelligence and cybercrime: implications for individuals and the healthcare sector," *The British Journal of Psychiatry*, vol. 225, no. 4, pp. 421–423, Oct. 2024, doi: 10.1192/bjp.2024.77.
- [29] K. Bonagiri, M. V. S. Nici, M. Gopalsamy, A. Iywaraya, R. R. H. Helan, and S. J. S., "AI-driven healthcare cyber-security: protecting patient data and medical devices," in *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, Aug. 2024, pp. 107–112, doi: 10.1109/ICoICI62503.2024.10696183.
- [30] N. Kshetri and J. Voas, "Agentic artificial intelligence for cyber threat management," *Computer*, vol. 58, no. 5, pp. 86–90, May 2025, doi: 10.1109/MC.2025.3544797.
- [31] M. Saadallah, A. Shahim, and S. Khapova, "Harmonizing paradoxical tensions in SOCs: a strategic model for integrating AI, automation, and human expertise in cyber defense and incident response," in *58th Hawaii International Conference on System Sciences (HICSS 2025)*, 2025, pp. 6171–6180, doi: 10.24251/HICSS.2025.738.
- [32] S. Jain, P. Ashok, and S. Prabhu, "Emerging technologies for cybersecurity in healthcare: evaluating risks and implementing standards," in *2024 International Conference on Cybernation and Computation (CYBERCOM)*, Nov. 2024, pp. 725–731, doi: 10.1109/CYBERCOM63683.2024.10803219.
- [33] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: anomaly detection and diagnosis from system logs through deep learning," in *2017 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 2017, pp. 1285–1298, doi: 10.1145/3133956.3134015.
- [34] R. H. Chowdhury, N. U. Prince, S. M. Abdullah, and L. A. Mim, "The role of predictive analytics in cybersecurity: detecting and preventing threats," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 1615–1623, Aug. 2024, doi: 10.30574/wjarr.2024.23.2.2494.
- [35] E. E. -Promise, G. Asante, F. Aina, H. Kure, and E. Gavua, "Leveraging artificial intelligence for predictive cybersecurity: enhancing threat forecasting and vulnerability management," *International Journal of Innovative Research in Advanced Engineering*, vol. 12, no. 2, Feb. 2024, doi: 10.26562/ijirae.2025.v1202.01.
- [36] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. F. -Sanz, and V. Pospelova, "The emerging threat of AI-driven cyber attacks: a review," *Applied Artificial Intelligence*, vol. 36, no. 1, Dec. 2022, doi: 10.1080/08839514.2022.2037254.
- [37] A. Gurtu and D. Lim, "Use of artificial intelligence (AI) in cybersecurity," in *Computer and Information Security Handbook*, 2025, pp. 1617–1624, doi: 10.1016/B978-0-443-13223-0.00101-6.
- [38] M. I. Khan, A. Arif, A. Raza, and A. Khan, "The most recent advances and uses of AI in cybersecurity," *Media Online*, vol. 3, pp. 566–578, 2024.
- [39] T. F. Blauth, O. J. Gstrein, and A. Zwitter, "Artificial intelligence crime: an overview of malicious use and abuse of AI," *IEEE Access*, vol. 10, pp. 77110–77122, 2022, doi: 10.1109/ACCESS.2022.3191790.
- [40] O. Beg, A. Khan, W. Rehman, and A. Hassan, "A review of AI-based cyber-attack detection and mitigation in microgrids," *Energies*, vol. 16, no. 22, Nov. 2023, doi: 10.3390/en16227644.
- [41] O. Arreche, T. R. Guntur, J. W. Roberts, and M. Abdullah, "E-XAI: evaluating black-box explainable AI frameworks for network intrusion detection," *IEEE Access*, vol. 12, pp. 23954–23988, 2024, doi: 10.1109/ACCESS.2024.3365140.

- [42] E. Sumartono, R. Harliyanto, S. M. T. Situmeang, D. S. Siagian, and E. Septaria, "The legal implications of data privacy laws, cybersecurity regulations, and AI ethics in a digital society," *The Journal of Academic Science*, vol. 1, no. 2, pp. 103–110, Jul. 2024, doi: 10.59613/29qypw51.
- [43] M. Durovic and T. Corno, "The privacy of emotions: from the GDPR to the AI Act, an overview of emotional AI regulation and the protection of privacy and personal data," in *Privacy, Data Protection and Data-driven Technologies*, London, United Kingdom: Routledge, 2024, pp. 368–404, doi: 10.4324/9781003502791-18.
- [44] A. Singhal, N. Neveditsin, H. Tanveer, and V. Mago, "Toward fairness, accountability, transparency, and ethics in AI for social media and health care: scoping review," *JMIR Medical Informatics*, vol. 12, Apr. 2024, doi: 10.2196/50048.
- [45] J. A. Balch, B. J. Evans, B. Shickel, A. Bihorac, G. R. Upchurch, and T. J. Loftus, "The dilemma of consent for AI in healthcare," *Surgey*, vol. 175, no. 5, pp. 1456–1457, May 2024, doi: 10.1016/j.surg.2024.01.019.
- [46] Y. Farid *et al.*, "Informed choices in the age of artificial intelligence," *Surgey*, vol. 175, no. 5, pp. 1454–1455, May 2024, doi: 10.1016/j.surg.2023.12.027.
- [47] F. M. Syed, E. S. F. Kousar, and E. Johnson, "AI-driven threat intelligence in healthcare cybersecurity," *Revista de Inteligencia Artificial en Medicina*, vol. 14, no. 1, pp. 431–59, 2023.
- [48] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems*, vol. 67, no. 8, pp. 6969–7055, Aug. 2025, doi: 10.1007/s10115-025-02429-y.
- [49] K. Ajeigbe and F. Wallace, "Interoperability and cybersecurity: ethical responsibilities of healthcare providers," *ResearchGate*, pp. 1–27, 2024.
- [50] P. Kashefi, Y. Kashefi, and A. G. Mirsarai, "Shaping the future of AI: balancing innovation and ethics in global regulation," *Uniform Law Review*, vol. 29, no. 3, pp. 524–548, Aug. 2024, doi: 10.1093/ulr/unae040.
- [51] S. M. Williamson and V. Prybutok, "Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare," *Applied Sciences*, vol. 14, no. 2, Jan. 2024, doi: 10.3390/app14020675.

BIOGRAPHIES OF AUTHORS



Rani Tiyas Budiyanthi    is an academic specializing in health law, health policy, and health ethics in Health Policy and Administration, Faculty of Public Health, Universitas Diponegoro, Indonesia. With a foundational education in medicine and a master's degree in health law, she possesses expertise in the analysis and development of policies concerning the legal and ethical dimensions of the medical field and public health. Her educational background includes a master's program in Health Law from the graduate program, Faculty of Law, Universitas Sebelas Maret, Indonesia; a professional degree from the Faculty of Medicine, Universitas Sebelas Maret, Indonesia; and a bachelor's degree from the undergraduate program, Faculty of Medicine, Universitas Sebelas Maret, Indonesia. She can be contacted at email: ranitiyas@lecturer.undip.ac.id.



Roro Isyawati Permata Ganggi    is scholarly expertise is centered on the field of digital humanities in the Library and Information Study Program, Faculty of Humanities, Universitas Diponegoro, Indonesia, with a particular emphasis on the documentation of intangible cultural heritage through multimedia, the cultural recognition of children, the psychological dimensions of information behavior within digital humanities, and the application of social media in this domain. Additionally, she is committed to fostering inclusivity in access to digital humanities. Her educational background is a bachelor's degree in Library and Information Science from UIN Sunan Kalijaga, Yogyakarta, Indonesia; and master's degree in Interdisciplinary Islamic Studies from UIN Sunan Kalijaga, Yogyakarta, Indonesia. She can be contacted at email: r.isyaganggi@gmail.com.