INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 9.47]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 12, Issue - 2, February - 2026

DOIs:10.2015/IJIRMF/202602018 --:-- Research Paper / Article / Review

Safeguarding AI-Driven Healthcare: Combating Data Poisoning Threats

[1]Shahazad Niwazi Qurashi, [2]Nasir A. Ali, [3]Ashraf Abdelmageid Ibrahim Khattab, [4]Wafa A. Hetany, [5]Farrukh Sobia

[1,4] Assistant Professor, Department of Public Health/Health Informatics Program, College of Nursing and Health Sciences / Jazan University, Jazan, Kingdom of Saudi Arabia
[2,3,4]Assistant Professor, Department of Public Health/Health Education and Promotion Program, College of Nursing and Health Sciences / Jazan University, Jazan, Kingdom of Saudi Arabia

[1]squrashi@jazanu.edu.sa, [2]naamohammed@jazanu.edu.sa, [3]aikhattab@jazanu.edu.sa,[4]whetany@jazanu.edu.sa, [5]fsobia@jazanu.edu.sa

Abstract: *The research emphasises the necessity of robust techniques to preserve the integrity of medical data, highlighting the growing threat of data poisoning in Artificial Intelligence (AI) systems used in the healthcare industry. Among the goals are assessing data poisoning methods as a defensive weapon, finding weaknesses, and suggesting technical and legislative fixes. Using databases such as Scopus and Web of Science, along with sophisticated analytical methods to identify patterns, the approach combines a qualitative and exploratory study with a systematic literature review (2017-2025). The findings showed a 39.5% rise in publications on the subject in 2023, stressing phishing (47%) as the major danger and data poisoning as a potential technique, along with firewalls and cybersecurity education. The combination of AI with methods like data poisoning, backed by legal frameworks (e.g., HIPAA, GDPR) and interdisciplinary cooperation, is seen as vital to reducing risks. All recommendations are looking at new technologies, including blockchain, developing specific policies for AI in healthcare, and investing in continuous training. Future lines of research should look at how effectively these tactics perform against evolving threats and how they impact patient privacy.*

Key Words: *Regulatory frameworks; healthcare security; Artificial Intelligence (AI); data poisoning*

1. INTRODUCTION:

To modernize the healthcare systems and with the concern of cyber threats and attacks, most of the countries around the world are focusing on and investing in digital health infrastructure. Digital health infrastructure refers to the integration of digital technologies into healthcare systems. This includes different technologies such as electronic health records, mobile health apps, wearable devices, and health information exchanges (Qurashi et al., 2025).In many cases, healthcare organizations find it rather difficult, as conventional security policies fail to meet these advanced attacks (Dahiya et al., 2022; May & Denecke, 2022). As the technology advances, the rapid digitisation of healthcare created more opportunities for cyber thieves (Acuna Acuna, 2023). These problems have been further compounded by a lack of advancement of strong security rules and an insufficiently qualified workforce that can handle such complex threats (Carreras & Finken, 2022; Newaz et al., 2021). In this context, nowadays, protecting healthcare data is an utmost legal and ethical need rather than just a technical one (Al Amin et al., 2023; Gupta et al., 2022). The consequences of security breaches range from stealing patients' information to modifying patients' diagnosis and treatment ((Hathaliya et al., 2022; Nemec Zlatolas et al., 2024). There is an urgent need to generate proactive cybersecurity policies. A remarkable approach, "the use of data poisoning methods", seems to be an inventive defensive method that has drawn attention to mitigate the threat of cybersecurity breach (Acuña Acuña, 2024; Guerrero–Sotelo et al., 2022).

This approach promises enhanced integrity, confidentiality, and availability of healthcare data, along with the ability to look for current vulnerabilities (Bernstam et al., 2022; Medina-Arco et al., 2024). A recent study emphasises AI's crucial role in reforming response to escalating threats and explores the interdependent relationship between generative AI and

cybersecurity and their applications in healthcare, so that healthcare facilities can predict and mitigate emerging risks by integrating AI into existing security infrastructure. The study outlined a total of five generative AI-based cybersecurity defence mechanisms that can be used to enhance digital infrastructure security in healthcare. These five mechanisms represent dynamic strategies that could revolutionise defensive capabilities from real-time anomaly detection to combating zero-day exploits (Qurashi et al., 2025). Hence, this study aims to discover the potential of data poisoning techniques to fortify the cybersecurity landscape with special reference to patient health information in the healthcare sector. By using an integrated theoretical and empirical approach, this study provides a systematic approach to technology, frameworks, and best practices in the domain of cybersecurity for the awareness of healthcare personnel. Furthermore, it evaluates and addresses developing cyber hazards in the environment based on industry trends, hence enabling the business to shift its paradigm toward a resilient strategy to the ongoing digital age cyber threats.

The following research questions were created for the development of the study. Evaluating how data poisoning techniques can be incorporated in cybersecurity strategies in healthcare facilities to protect patient health information and ensure the data integrity of the clinical information system. Thus, the outcome of the current study aims to offer the required information on the use of data learning technology as an efficient tool to safeguard organisations and to be able to create the required foundations to design a cybersecurity strategy integrated into the computer systems of health institutions.

2. METHODOLOGY:

This study uses an integrated methodological framework that combines thorough literature analysis with a qualitative, exploratory, cross-sectional approach. Based on theoretical ideas by Singh et al. (2024); van Leersum and Maathuis (2025), we have investigated how data poisoning strategies could prevent and neutralize dangers, hence protecting crucial patient health information. A thorough literature analysis with the MeSH terms “data poisoning” and “AI preventative strategies” within the “healthcare cyber security” was done, and the relevant publications ranging from the year 2017 to 2025 were sorted out. This selection process adheres to Munkøe et al. (2022) methodological guidelines to consolidate and critique the evolution of practices and ideas in this specialised subject. Selection criteria were to include the studies those offering major insights on AI applications in healthcare and cybersecurity. Primary academic sources such as Web of Science, Emerald, Scopus, Science Direct, and EBSCO host were utilized under precisely specified search terms. This step ensures the collection of pertinent data relevant to the study.

Analysis and synthesis of data

Based on the selection criteria for searching relevant studies, the number of research articles obtained from various databases has been summarised in the following Table 2.1. This approach allowed for the identification of important characteristics like impact, privacy, data, discrimination, and decision-making, therefore allowing efficient information triangulation.

Table 2.1: Matrix of contrasting findings

Database	Search Criteria	Articles
Web of Science, Emerald, Scopus, Science Direct, EBSCOhost, and English-language Internet Sites	"Data poisoning in healthcare" + "AI prevention strategies"+ “healthcare cybersecurity” + "articles only"	160
Web of Science, Emerald, Scopus, Science Direct, EBSCOhost, and Spanish-language Internet Sites	"Data poisoning" + "Health security" + "articles only"	20

The results and conclusion parts of these articles were carefully evaluated and synthesized after data centralization for the traits and affecting elements of data poisoning in healthcare cybersecurity. This step focused on highlighting trends, disputes, and related threats.

Incorporation of sophisticated analytical tools

In these articles, the advanced technologies were used to display and examine patterns, including graphs showing the growing emphasis on digital health security research indexed in databases like Scopus and Web of Science.

Rationale for the qualitative method

Susanto et al. (2024) suggested the need to investigate complex settings within healthcare cybersecurity through the qualitative approach. This method combined the multidisciplinary points of view from informatics, ethics, and health with an in-depth analysis of defensive strategies, including data poisoning.

Anticipated results and field contributions

Triangulation of the collected data revealed trends and possibilities, especially in methods like data poisoning, highlighting the need to include regulatory and pedagogical approaches to strengthen technology infrastructures in healthcare. An strong ethical and legal framework should support the adaptation of defences according to Calderón Urriola and Argota Pérez (2023). This scientific approach greatly advances the area with evidence-based solutions to protect sensitive data and preserve a safe clinical environment, hence offering a holistic viewpoint on trends and issues in healthcare cybersecurity.

3. DISCUSSION & RESULTS:

The rising focus on "data poisoning" as a concept within healthcare cybersecurity underscores the necessity for innovative defensive strategies to combat digital threats to health systems (Table 3.1). The keywords for search were combining "data poisoning," "health," and "cybersecurity", which clearly reflects a growing demand for specialized strategies to enhance health system defences against cyber threats. This interest is supported by the research contributions of Al Khatib et al. (2024); Czekster et al. (2025); Snigdha et al. (2025), who identified early the cybersecurity risks in medical environments. Studies also provide methods of enhancing cybersecurity, especially suited for the healthcare industry (Kuo and Horn (2023); Munkøe et al. (2022) .

Table 3.1: Search results of the study object

Year	Articles	Percentage
2017	5	1.25%
2018	12	3.00%
2019	25	6.25%
2020	35	8.75%
2021	70	17.50%
2022	103	25.50%
2023	150	39.50%
2024	115	23.25%
2025	121	31.00%

Yearly data insight

Table 3.1 shows a steady rise in the number of papers concentrating on data poisoning from 2017 to 2025, showing a strong awareness of its possible utility in safeguarding against cyber risks in healthcare. Reflecting in Table 3.2, the even spread of literature reviews, case studies, and empirical studies points to a complete analysis of data poisoning in healthcare cybersecurity, suggesting a careful look at current practices and new approaches to protect vital patient data.

Table 3.2: Identified scientific studies

Study type	Articles	Percentage
Literature review	40	40%
Case studies	30	30%
Empirical	30	30%

Scientific literature insights in Table 3.2 show that 40% of investigations are literature reviews; case studies and empirical studies each make up 30%. This emphasises the need to create strong regulatory systems and data quality controls to improve security by underlining a wide approach to comprehending the application and effectiveness of data poisoning in healthcare cybersecurity, therefore complementing the issues as highlighted by Al Khatib et al. (2024).

Development of cyberattack complexity

The paper underlines how cyber-attacks have changed from phishing to more complex methods like malware because of their covert penetration powers (da Cruz (2025); Kuo and Horn (2023). Recently, the thorough preventative plans have been suggested by combining technological tools such as encryption and two-factor authentication with ongoing cybersecurity education (Munkøe et al. (2022); Singh et al. (2025).

Impact and compliance

The study shows how cyberattacks affect patient privacy and safety beyond financial loss. Following laws like the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Rights (GDPR) is vital as it promotes ethical behaviour to safeguard patient rights and data integrity.

Focusing on data corruption and AI

The increasing use of AI in medicine highlights the importance of being ready for cybersecurity issues. Creating safe medical settings calls for cooperation across many industries. The study concludes by evaluating data poisoning as a protective measure for AI systems in healthcare, underscoring the urgent need for robust cybersecurity methodologies in an increasingly digital health world (Balasubramanian et al. (2025); Liu et al. (2024). Table 3.3 provides an overview of research publication growth in AI and cybersecurity, highlighting the rising concern for data security driven by innovations in the medical field.

Table 3.3: Distribution of publications by year

Year	Number of Publications	Percentage
2009	1	1.56%
2016	1	1.56%
2019	2	3.14%
2020	1	1.56%
2021	5	7.81%
2022	20	31.25%
2023	29	45.31%
2024	35	57.81%
2025	41	46.70%

Technology and security innovation

Table 3.4 shows the priorities of the research areas, such as data mining for security, highlighting its role in preventing unauthorised data breaches. Moreover, it emphasises data mining's critical role in developing early warning systems to protect patient data from unauthorized access.

Defence against various cyber threats

1. Data mining: Amer et al. (2025) and Brilhante et al. (2023) explored advanced data mining as a fundamental aspect of warning systems that protect patient data.
2. IoT and biomedical security: El-Saleh et al. (2025) and Gómez de Ágreda et al. (2021) focused on the IoT's crucial role in securing biomedical devices from intrusion attempts.
3. AI for cyber defence: Aditya et al. (2025) and Raja (2025) focused on AI's use to develop advanced defence systems capable of pre-empting and neutralising cyber threats before compromising health data.

Detected data trends

Table 3.5 shows personal information and medical records as the primary data types extracted in cyberattacks, highlighting the urgent need to protect these crucial assets.

Table 3.5: Most extracted data in cyberattacks on the health sector

Type of data	Percentage
Personal information	42%
Medical records	37%
Insurance information	19%
Payment data	15%

Research scope

The literature highlights data poisoning as a crucial defensive strategy against health information theft. According to Pawlicka et al. (2021), multidisciplinary collaboration is essential for a holistic approach to healthcare cybersecurity, integrating medical, technical, and information security insights to construct effective defences against cyber threats.

Table 3.4: Panorama of technological innovation in digital health

Topics	Importance
Data mining	Medium
Internet of Things (IoT) for biomedical products	Medium
Cybersecurity in health	High
AI in health	High
Legislative harmonization	Medium
Machine learning	Low
Detection of phishing attacks	Low
Detection of SQL injections	Low
AI for smart cities	Medium
Adversarial attacks against AI	Medium

Defence approaches in healthcare

Table 3.6 outlines common defence strategies like data poisoning and education initiatives fundamental to comprehensive digital defence, emphasizing a multidimensional approach to cybersecurity in healthcare, as advocated by influential cyber experts (Health–Americas, 2024).

Table 3.6: Main defences against cyberattacks in healthcare centers

Defense Strategy	Description	Examples of Tools
Data Poisoning	Inserting false data to confuse attackers	Synthetic data sets
Web Application Firewalls (WAF)	Monitoring and filtering the HyperText Transfer Protocol (HTTP) traffic between a web application and the Internet	ModSecurity, Cloudflare
Antivirus programs	Detecting and removing malware from computers and networks	Norton, McAfee
eXtended Detection and Response (XDR)	Unified security monitoring and incident response across all security layers	Cisco SecureX, Palo Alto Networks
Cybersecurity education	Training staff on best practices and threat awareness	Online courses, workshops

Common cyberattack techniques

According to Table 3.7, phishing holds a 47% frequency in attacks, urging urgent implementation of improved security measures and staff training to combat emerging threats.

Table 3.7: Common tools used in cyberattacks on the health sector

Type of attack	Frequency (%)
Phishing	47%
Malware	36%
Interception (MitM)	13%
Social Engineering	16%

Essentially, this paper offers a methodical framework for healthcare cybersecurity emphasizing the combination of data poisoning and AI as clear solutions to thoroughly fight and reduce digital risks, supported by practical data and academic agreement.

The fast digitalization of the healthcare industry calls for implementing more complex and focused approaches to prevent cyberattacks, hence surpassing conventional security measures (Kuo and Horn (2023). Pawlicka et al. (2021) underlined the need to include sophisticated techniques like data poisoning, which seeks to confuse attackers and protect critical patient data efficiently. This paper underlines the pressing need to improve threat detection capacity and apply strong mitigation plans. These include the development of creative technologies and the implementation of a comprehensive regulatory system, especially meant for the use of AI in the medical sector.

This study underlines the need to develop and use innovative technologies to provide a consistent and safe treatment environment, also supported by Bernstam et al. (2022) and Medina-Arco et al. (2024). Highlighting this as a crucial barrier against hostile assaults, a strong digital infrastructure preserves the integrity of healthcare information systems.

This perspective meets the need to use appropriate security policies to govern the problems brought on by the combination of AI and healthcare services.
Data poisoning is one technique that not only increases confidence in the security of medical data but also helps prevent identity theft and illegal data extraction. The report advocates building a better clinical environment using present cybersecurity technology, like improved threat detection systems and thorough regulatory frameworks meant for AI in healthcare. By adopting such a consistent strategy, the healthcare industry will be able to preserve confidence and security in clinical data management and reinforce its defenses against always-changing cyber threats.

4. CONCLUSION:

This research emphasizes the growing relevance and use of data poisoning as a basic preventative tool in health information system cybersecurity. Apart from changing conventional medical practices, the healthcare industry's growing usage of AI is enhancing security measures, thereby requiring the creation and use of sophisticated technologies, including data poisoning. Also, data poisoning is significant as a preventive action to protect healthcare information systems. Apart from changing traditional medical procedures, the healthcare industry's growing usage of AI is greatly enhancing cybersecurity measures. Data poisoning is a proactive and effective strategy needed to protect the confidentiality and integrity of patient data when used appropriately in AI systems. This creative concept drives intentional data insertion in reaction to perceived hostile behaviour. Increasing the price to assailants under this idea acts as a deterrent and helps to stop the illegal gathering of vital information.
A comprehensive strategy and multidisciplinary cooperation with AI specialists, cybersecurity authorities, and medical professionals will thus ensure the effective execution of data poisoning. This constructive collaboration ensures the quality of patient treatment and does not compromise the operational efficiency of healthcare systems. Healthcare businesses also must budget to raise the knowledge and management of present and future cyber threats using staff members' ongoing professional development. Understanding patient information security needs drives regular upgrades and a comprehensive knowledge of security rules, including data poisoning.
Ultimately, data poisoning is a significant evolution in safeguarding healthcare information systems against many assaults. This strategy might enable the healthcare sector to be more resistant to attacks, hence ensuring the protection of patient data and enhancing the overall resilience of the healthcare. Given a culture where digital technologies are quickly changing healthcare, security policies must always be updated and adjusted to balance the sophisticated cyber risks of our day, including data poisoning.

Acknowledgment: The authors would like to thank the Department of Public Health, College of Nursing and Health Sciences, Jazan University, Jazan, Kingdom of Saudi Arabia, for providing laboratory support and infrastructure to carry out this research work.

Author's Contributions: SNQ conceptualised the study, performed the analysis, and prepared the research summary. NAA and AAIK **c**hecked the formatting and rectified the error, WH interpreted the result and prepared of the revised manuscript draft and FS prepared the first draft of the manuscript. All authors checked and approved the manuscript for publication.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES:

1. Acuña Acuña, E. G. (2023). Aplicación de minería de datos e Internet de las cosas (IoT) para productos biomédicos. *Revista Internacional Tecnología, Ciencia y Sociedad*, *13*(1). https://doi.org/10.37467/revtechno.v12.3444
2. Acuña Acuña, E. G. (2024). Healthcare Cybersecurity: Data Poisoning in the Age of AI. *Journal of Comprehensive Business Administration Research*. https://doi.org/10.47852/bonviewJCBAR42024067
3. Aditya, S. D., Wadjdi, A. F., & Rimbawa, D. (2025). Enhancing Cyber Defense Capabilities through AI Technology. *East Asian Journal of Multidisciplinary Research*, *4*(3), 985-1004. https://doi.org/10.55927/eajmr.v4i3.85
4. Al Amin, A., Hong, J., Bui, V.-H., & Su, W. (2023). Emerging 6G/B6G wireless communication for the power infrastructure in smart cities: Innovations, challenges, and future perspectives. *Algorithms*, *16*(10), 474. https://doi.org/10.3390/a16100474

5. Al Khatib, I., Shamayleh, A., & Ndiaye, M. (2024). Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. *Informatics*, *11*(3), 47. https://doi.org/10.3390/informatics11030047
6. Amer, S., Hazim, R., & Kader, W. (2025). Data Mining and Machine Learning-Based Healthcare Monitoring in Cloud-IoT. *Mesopotamian Journal of CyberSecurity*, *5*(1), 39-61. https://doi.org/10.58496/MJCS/2025/004
7. Balasubramanian, S., Shukla, V., Islam, N., Upadhyay, A., & Duong, L. (2025). Applying artificial intelligence in healthcare: lessons from the COVID-19 pandemic. *International journal of production research*, *63*(2), 594-627. https://doi.org/10.1080/00207543.2023.2263102
8. Bernstam, E. V., Shireman, P. K., Meric-Bernstam, F., N Zozus, M., Jiang, X., Brimhall, B. B., Windham, A. K., Schmidt, S., Visweswaran, S., & Ye, Y. (2022). Artificial intelligence in clinical and translational science: Successes, challenges and opportunities. *Clinical and translational science*, *15*(2), 309-321. https://doi.org/10.1111/cts.13175
9. Brilhante, D. d. S., Manjarres, J. C., Moreira, R., de Oliveira Veiga, L., de Rezende, J. F., Müller, F., Klautau, A., Leonel Mendes, L., & P. de Figueiredo, F. A. (2023). A literature survey on AI-aided beamforming and beam management for 5G and 6G systems. *Sensors*, *23*(9), 4359. https://doi.org/10.3390/s23094359
10. Calderón Urriola, N. F., & Argota Pérez, G. (2023). Competitividad desde el pensamiento complejo y rizomático mediante ingeniería en ciencias de datos no computacional. *Revista Campus*, *28*(35), 35–44. https://doi.org/10.24265/campus.2023.v28n35.03
11. Carreras, B. N., & Finken, S. (2022). Autonomy Alliances and Data Care Practices. 47-57. https://doi.org/10.1007/978-3-031-15688-5_5 (Human Choice and Digital by Default: Autonomy vs Digital Determination)
12. Czekster, R. M., Webber, T., Furstenau, L. B., & Marcon, C. (2025). Dynamic risk assessment approach for analysing cyber security events in medical IoT networks. *Internet of Things*, *29*, 101437. https://doi.org/10.1016/j.iot.2024.101437
13. da Cruz, J. d. A. (2025). Chapter 103 - Future Trends for Cyber Attacks in the Healthcare Industry. In J. R. Vacca (Ed.), *Computer and Information Security Handbook (Fourth Edition)* (pp. 1651-1661). Morgan Kaufmann. https://doi.org/https://doi.org/10.1016/B978-0-443-13223-0.00103-X
14. Dahiya, M., Nitin, N., & Dahiya, D. (2022). Intelligent cyber security framework based on SC-AJSO feature selection and HT-RLSTM attack detection. *Applied sciences*, *12*(13), 6314. https://doi.org/10.3390/app12136314
15. El-Saleh, A. A., Sheikh, A. M., Albreem, M. A. M., & Honnurvali, M. S. (2025). The Internet of Medical Things (IoMT): opportunities and challenges. *Wireless Networks*, *31*(1), 327-344. https://doi.org/10.1007/s11276-024-03764-8
16. Gómez de Ágreda, Á., Feijoo González, C. A., & Salazar García, I. A. (2021). Una nueva taxonomía del uso de la imagen en la conformación interesada del relato digital. Deep fakes e inteligencia artificial. *El profesional de la información*, *30*(2), 1-24. https://doi.org/10.3145/epi.2021.mar.16
17. Guerrero–Sotelo, R., Orellana-Centeno, J. E., & Orozco–Reséndiz, A. C. (2022). Los biodatos del expediente clínico odontológico en México: análisis jurídico y bioético. *Acta Odontológica Colombiana*, *12*(2), 91-104. https://doi.org/10.15446/aoc.v12n2.98723
18. Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S. M., & Huang, K.-Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. *Sensors*, *22*(5), 2017. https://doi.org/10.3390/s22052017
19. Hathaliya, J. J., Tanwar, S., & Sharma, P. (2022). Adversarial learning techniques for security and privacy preservation: A comprehensive review. *Security and Privacy*, *5*(3), 1-46. https://doi.org/10.1002/spy2.209
20. Health–Americas, T. L. R. (2024). Corruption: possibly the biggest threat to health care. *Lancet Regional Health-Americas*, *32*, 100744. https://doi.org/10.1016/j.lana.2024.100744
21. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016
22. Kuo, P.-Y., & Horn, M. S. (2023). EcoSanté Lifestyle Intervention: Encourage Reflections on the Connections between Health and Environment. *ACM Transactions on Computer-Human Interaction*, *30*(6), 1-37. https://doi.org/10.1145/3609325
23. Liu, S., Wang, Z., Kumari, S., Lv, J., & Chen, C. M. (2024). Provably Secure Anti-Phishing Scheme for Medical Information in Smart Healthcare. *IEEE Internet of Things Journal*, *11*(23), 38086-38097. https://doi.org/10.1109/JIOT.2024.3445375

24. May, R., & Denecke, K. (2022). Security, privacy, and healthcare-related conversational agents: a scoping review. *Informatics for Health and Social Care*, *47*(2), 194-210. https://doi.org/10.1080/17538157.2021.1983578
25. Medina-Arco, J. G., Magán-Carrión, R., Rodríguez-Gómez, R. A., & García-Teodoro, P. (2024). Methodology for the Detection of Contaminated Training Datasets for Machine Learning-Based Network Intrusion-Detection Systems. *Sensors*, *24*(2), 479. https://doi.org/10.3390/s24020479
26. Munkøe, M., Mölder, H., & Gil, M. G. (2022). La ciberseguridad en la era de hipercompetitividad. *Revista CIDOB d'Afers Internacionals*(131), 69-94. https://doi.org/10.24241/rcai.2022.131.2.69
27. Nemec Zlatolas, L., Welzer, T., & Lhotska, L. (2024). Data breaches in healthcare: security mechanisms for attack mitigation. *Cluster Computing*, *27*(7), 8639-8654. https://doi.org/10.1007/s10586-024-04507-2
28. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, *2*(3), 1-44. https://doi.org/10.1145/3453176
29. Pawlicka, A., Pawlicki, M., Kozik, R., & Choraś, R. S. (2021). A systematic review of recommender systems and their applications in cybersecurity. *Sensors*, *21*(15), 5248. https://doi.org/10.3390/s21155248
30. Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *6*(1), 438-462. https://doi.org/10.60087/jaigs.v6i1.268
31. Raja, R. S. (2025). "SQLSynthGen: Generating Synthetic Data for Healthcare Databases". *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, 1-11. https://doi.org/10.1109/ICAIC63015.2025.10849122
32. Singh, C., Singh, R., Kamini, & Kumar, Y. (2025). Exploring Cybersecurity in Healthcare Systems: A Systematic Review. In A. Choudhury, K. Kaushik, V. Kumar, & B. K. Singh (Eds.), *Cyber-Physical Systems Security: A Multi-disciplinary Approach* (pp. 119-149). Springer Nature Singapore. https://doi.org/https://doi.org/10.1007/978-981-97-5734-3_6
33. Singh, N., Jain, M., Kamal, M. M., Bodhi, R., & Gupta, B. (2024). Technological paradoxes and artificial intelligence implementation in healthcare. An application of paradox theory. *Technological Forecasting and Social Change*, *198*, 122967. https://doi.org/10.1016/j.techfore.2023.122967
34. Snigdha, E. Z., Jalil, M. S., Dahwal, F. M., Saeed, M., Mehedy, M. T. J., & Hasan, S. K. (2025). Cybersecurity in Healthcare IT Systems: Business Risk Management and Data Privacy Strategies. *The American Journal of Engineering and Technology*, *7*(03), 163-184. https://doi.org/10.37547/tajet/Volume07Issue03-15
35. Susanto, P. C., Yuntina, L., Saribanon, E., Soehaditama, J. P., & Liana, E. (2024). Qualitative method concepts: Literature review, focus group discussion, ethnography and grounded theory. *Siber Journal of Advanced Multidisciplinary*, *2*(2), 262-275. https://doi.org/10.38035/sjam.v2i2.207
36. van Leersum, C. M., & Maathuis, C. (2025). Human centred explainable AI decision-making in healthcare. *Journal of Responsible Technology*, *21*, 100108. https://doi.org/10.1016/j.jrt.2025.100108
37. Qurashi, S. N., Sobia, F., Hetany, W. A., & Sultan, H. (2025). Enhancing Cybersecurity Defenses in Healthcare Using AI: A Pivotal Role in Fortifying Digital Health Infrastructure. *Medinformatics*, *2*(4), 268–278. https://doi.org/10.47852/bonviewMEDIN52024121.