Received: 9 August 2024 | Revised: 23 September 2024 | Accepted: 8 October 2024 | Published online: 17 October 2024

RESEARCH ARTICLE

Journal of Comprehensive Business Administration Research
2024, Vol. 00(00) 1–10
DOI: 10.47852/bonviewJCBAR42024067

BON VIEW PUBLISHING

Healthcare Cybersecurity: Data Poisoning in the Age of AI

Edwin Gerardo Acuña Acuña[1,*]

[1]*Department of Engineering, Universidad Latinoamericana de Ciencia y Tecnología, Costa Rica*

Abstract: This study focuses on the challenges the healthcare sector faces in the wake of increasing digitalization, particularly the growing threat of data poisoning in artificial intelligence systems. Unlike other research, this work delves into the current security protocol weaknesses, highlighting the specific vulnerabilities of healthcare systems and the urgent need for innovative solutions to protect both patients and institutions. Throughout the research, key gaps in security mechanisms are identified and analyzed, showing how these flaws can be exploited by attackers to compromise sensitive information, undermining trust in digital healthcare tools. The methodology combines existing theories with real-world data, allowing for an in-depth and detailed analysis of the risks posed by data poisoning.

Advanced cybersecurity strategies are presented, emphasizing the importance of multi-layered detection and mitigation systems designed specifically for the healthcare sector's needs. Additionally, the broader impact these cybersecurity challenges could have on business processes is explored, revealing how they might slow down the essential digital transformation required to enhance modern healthcare services. This study not only sheds light on security issues in the healthcare sector but also offers practical recommendations to strengthen current defenses. In conclusion, it calls for urgent action to develop new technologies and enforce stricter regulations that safeguard data integrity and ensure a safe and successful digital transition in the face of emerging cybersecurity threats.

Keywords: data poisoning, artificial intelligence, cybersecurity, privacy

1. Introduction

The rapid integration of artificial intelligence (AI) into healthcare is reshaping how diagnostics and treatments are carried out, offering incredible opportunities for more personalized and efficient care. However, as Dahiya et al. [1] point out, this technological progress comes with significant risks, particularly regarding the security of patient data and the growing threat of identity theft—a concern that Acuña [2] emphasizes as especially pressing. As the healthcare industry continues its digital transformation, the fusion of AI with business processes not only boosts operational efficiency but also opens the door to new vulnerabilities that require urgent attention.

In recent years, there has been a notable increase in cyberattacks, including advanced methods such as Man-in-the-Middle (MitM) tactics. These attacks have compromised the integrity of AI-based systems and the confidentiality of patient information, further exacerbating these threats. The situation is made more complex by the apparent lack of effective mitigation strategies, a critical shortfall identified by López-Aguilar et al. [3]. This underscores the urgent need to bolster defenses against these emerging dangers.

Recent statistics provided by the Organization for Economic Co-operation and Development and the World Health Organization, as cited by Hussmann [4], reveal that as many as 60% of healthcare institutions have experienced security breaches over the past year. This alarming trend is further illustrated by reports from the Ministry of Justice, referenced by Gil Membrado [5], which emphasize that despite the benefits of technological advancements, these have paradoxically increased the vulnerability of healthcare systems. As the pace of digital transformation accelerates, these vulnerabilities are becoming more pronounced, highlighting the urgent need for more robust cybersecurity measures.

The constant evolution of cyber threats has driven researchers like Al Amin et al. [6] and Gupta et al. [7] to investigate new strategies for both offensive and defensive cybersecurity measures. Their work highlights the pressing need for greater vigilance and the development of advanced detection techniques. Additionally, international collaboration in cybersecurity, as emphasized by Hathaliya et al. [8], and the adaptation of security policies to address these emerging technological challenges, as suggested by Guerrero-Sotelo et al. [9], are essential for building a coordinated and effective defense.

In pioneering research, Bernstam et al. [10] and Medina-Arco et al. [11] introduce data poisoning as a vital technique to reinforce the confidentiality, integrity, and availability of information within AI systems. Their findings suggest that data poisoning plays a pivotal role in preventing unauthorized access and protecting against the manipulation of sensitive data. Matsuzaka and Yashiro [12] support this perspective, arguing that the integration of data poisoning with AI significantly bolsters the security of healthcare data. This view is further echoed by Calderón Urriola and Argota Pérez [13] as well as Cirio et al. [14], who advocate for adapting security strategies to address the continuously evolving threats in this domain.

This study focuses on the pressing issue of cybersecurity within the ongoing digital transformation in healthcare. It explores how data poisoning can be used as an effective tool to bolster information

*Corresponding author: Edwin Gerardo Acuña Acuña, Department of Engineering, Universidad Latinoamericana de Ciencia y Tecnología, Costa Rica. Email: eacunaa711@ulacit.ed.cr

protection, emphasizing the need to strengthen digital security measures to safeguard both patient data and healthcare professionals as they navigate an increasingly AI-driven environment. Sabouri et al. [15] and Rugo et al. [16] point to data poisoning as a crucial proactive approach in cybersecurity. Meanwhile, the integration of deep learning into security systems, as demonstrated by Ayma Quirita et al. [17] and Giambelluca [18], plays a key role in detecting unusual behaviors and reinforcing strategies like data poisoning, ultimately strengthening cybersecurity and protecting sensitive patient information.

As technological transformation progresses, specific vulnerabilities within healthcare systems have been exposed, as reported by Brilhante et al. [19] as well as Gómez-de-Ágreda et al. [20]. This exposure underscores the importance of adopting a proactive approach to understanding and mitigating the risks associated with AI applications, as emphasized by Akhtar et al. [21] as well as Sánchez and Rojas [22]. The challenges identified in healthcare cybersecurity necessitate a comprehensive strategy that, according to Salmi and Bogucka [23], must harmonize technological innovations with human and regulatory elements. This approach also involves ongoing education for healthcare personnel and the enhancement of technological infrastructures, both of which are essential for ensuring effective and enduring protection against the diverse and evolving landscape of cyber threats. Rojas Buenaño [24] further emphasizes the need for clear policies and well-defined security practices, specifically tailored to the healthcare environment, to effectively address both emerging and established risks.

Interdisciplinary collaboration plays a key role in this strategy, blending technical expertise with clinical insights, as noted by Saini and Saxena [25] as well as Das et al. [26]. This integration greatly improves the healthcare sector's capacity to predict, respond to, and recover from cyberattacks, helping to maintain both the continuity and quality of medical care. In the increasingly complex landscape of healthcare cybersecurity, various incidents underscore the growing severity of threats. For instance, Li et al. [27] detail an incident where a healthcare system was compromised by a ransomware attack, stressing the critical need for secure backups and comprehensive cybersecurity training. Similarly, Acuña [28] reports on a phishing incident at a hospital, pointing out deficiencies in security protocols and underscoring the essential role of continuous staff education. Furthermore, Marin et al. [29] describe a Man-in-the-Middle attack that jeopardized communication between medical devices, while Singh et al. [30] document a case of SQL injection that compromised medical records. Additionally, Ding et al. [31] discuss the misuse of AI leading to incorrect data classifications, emphasizing the necessity for robust and validated AI systems.

Roldán Álvarez and Vargas Montoya [32] highlight the importance of flexible and effective cybersecurity governance in healthcare, showing how clear policies and procedures can greatly reduce the risks of cyberattacks and data breaches. In a similar context, Qahri-Saremi and Turel [33] explore the trend of targeted and sophisticated attacks exploiting vulnerabilities in health information systems, underscoring the critical need for constant vigilance and ongoing enhancements in cybersecurity measures. Sheehan et al. [34] provide insights into the evolution of cybercriminal tactics, advocating for adaptation and continuous learning as key defenses to protect sensitive health information assets.

Palencia-Díaz and de Jesús Palencia-Vizcarra [35] highlight how these interconnected examples not only reveal the variety and seriousness of cyber threats in the healthcare sector but also stress the need to address these vulnerabilities with urgency. Adopting a comprehensive, multidisciplinary approach to cybersecurity is essential to safeguard the integrity, availability, and confidentiality of crucial medical information, a point strongly backed by Sarajchi and Sirlantzis [36]. Mora Pineda [37] also emphasizes the increasing importance of maintaining a sustained, focused commitment to cybersecurity in healthcare. This approach requires blending technical expertise with a deep understanding of clinical environments and healthcare operations, underscoring the need for a holistic strategy to protect healthcare infrastructure from growing digital threats.

2. Methodology

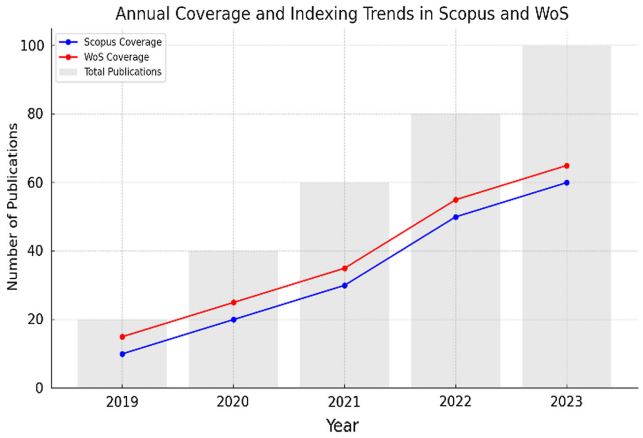
In this study, we employ a meticulously integrated methodology that synthesizes a comprehensive literature review with a descriptive, exploratory, non-experimental, and cross-sectional qualitative approach. This methodological design is intentionally crafted to identify effective preventive strategies and to thoroughly examine data poisoning as a defensive mechanism against cyberattacks within healthcare systems. Drawing on the robust theoretical framework established by Francisco Ávila-Tomás et al. [38], our primary objective is to investigate how data poisoning tactics can effectively impede and neutralize potential threats, thereby safeguarding critical patient information. The qualitative nature of this methodology is essential for achieving a deep and nuanced understanding of the specific dynamics and contexts in which these defensive strategies are applied, allowing for a comprehensive and in-depth exploration of the subject matter.

To achieve this, a systematic literature review will be conducted, meticulously selecting relevant publications from the period between 2017 and 2023 that focus on the intersection of data poisoning and preventive strategies within the healthcare context. The rationale for adopting this methodological approach lies in the necessity to synthesize and critically examine the evolution of both practices and theoretical perspectives in this highly specialized field. As noted by Nappa et al. [39], conducting a documentary review is crucial for obtaining a thorough understanding of the current and emerging dynamics in cybersecurity, particularly within the unique challenges presented by healthcare settings. This approach ensures that we gain a comprehensive grasp of the multifaceted challenges and potential solutions related to the protection of sensitive health information.

The literature review process will prioritize studies based on their relevance and contribution to the specific objectives of our research, with particular emphasis on those that offer significant insights into cybersecurity measures and the application of AI within medical contexts. For the selection and analysis of references, we will utilize primary academic databases such as Web of Science, Emerald, Scopus, Science Direct, and EBSCOhost. Our search strategy will involve the use of carefully chosen keywords, including 'data poisoning in health,' 'prevention strategies in AI,' and 'cybersecurity in medical care.' This rigorous and systematic approach to data collection ensures that our understanding of the researched themes is both comprehensive and accurate, providing a solid foundation for the study.

The evaluation and synthesis of the information gathered through this extensive literature review will play a pivotal role in addressing the critical research questions posed by Munkøe and Mölder [40]. The in-depth analysis of the literature has provided valuable insights into the cybersecurity strategies currently employed in the healthcare sector, with a particular focus on data drawn exclusively from academic sources and specialized publications. Following the recommendations of Parra et al. [41], the integration and synthesis of these bibliographic findings have enabled the development of practical and evidence-based recommendations that are grounded in expert-validated theories. This methodological approach firmly substantiates the use of a

Figure 1
Growth trends in the indexing of research on digital health security in Scopus and Web of Science



literature review as a key component of the research, ensuring that the conclusions and recommendations presented are deeply anchored in current and relevant research, thus providing a robust and reliable foundation for further exploration (see Figure 1).

Once the sources were carefully compiled, a detailed contrast matrix was developed to systematically organize the identified literature based on the specific databases from which they were obtained (as shown in Table 1). This matrix was essential for categorizing and comparing the studies, providing a structured framework for an in-depth analysis of the gathered data.

Following the creation of the matrix, the data were centralized and thoroughly analyzed, with special emphasis on identifying and extracting key descriptors such as impact, discrimination, data privacy, and decision-making processes. These descriptors were selected for their relevance to the study's goals and their importance within the broader context of cybersecurity and AI in healthcare. By honing in on these critical aspects, the analysis was able to uncover nuanced insights and establish correlations among the various sources, thereby enriching the overall research findings.

This approach allowed for a thorough review of the literature, helping to uncover patterns and highlight gaps in the current knowledge. As a result, it enabled more accurate and insightful conclusions, providing a deeper understanding of the complex challenges surrounding data poisoning and cybersecurity in healthcare systems.

After gathering all the data, the main characteristics and factors linked to data poisoning in healthcare cybersecurity were carefully identified and analyzed. This detailed examination shed light on the key aspects of data poisoning, while also revealing broader trends in AI cybersecurity.

Table 1
Matrix of contrasting findings

Database	Search criteria	Articles
Web of Science, Emerald, Scopus, Science Direct, EBSCOhost, and English-language Internet Sites	"Data poisoning" + "Health security" + "articles only"	120
Web of Science, Emerald, Scopus, Science Direct, EBSCOhost, and Spanish-language Internet Sites	"Data poisoning" + "Health security" + "articles only"	40

These trends pose significant challenges but also offer unique opportunities in the digital age. Through this method, important debates, critical threats, and key discussions surrounding data poisoning in healthcare were uncovered. The analysis is further enriched by the contributions of researchers like Kuo and Horn [42] as well as Zare et al. [43], who highlight the ongoing evolution of ethical approaches to data poisoning and cybersecurity in healthcare.

The proposed multilayer network model takes into account the dynamic and evolving nature of AI technologies by integrating copula nodes, which act as critical points within the network structure, enabling adaptation to new threats and vulnerabilities. However, the model could benefit from incorporating more advanced or emerging AI paradigms, such as reinforcement learning or generative AI, which would allow for a more flexible and proactive response to evolving threats. While copula nodes are fundamental to this model, it is crucial to provide more clarity on how they are operationalized in real-world scenarios. These nodes are essential for coordinating interactions between the different layers of the network, but their practical application may face limitations or restrictions, such as scalability and interoperability with existing systems, that the article does not address in detail.

In addition to textual analysis, a visual examination was conducted to align with the research objectives. This visual analysis focused on the expanding field of cybersecurity in healthcare, with particular attention to data poisoning. Reflecting the observations of Muñoz-del-Carpio-Toia et al. [44], there has been a notable increase in scholarly literature emphasizing the need to evaluate strategies for combating identity theft and data misappropriation in healthcare. This surge in academic attention, as underscored by Shalev-Shwartz and Ben-David [45], bolsters the development of evidence-based tactics and validated practices aimed at improving data security. The methodological framework employed in this study involves a systematic documentary review, designed to scrutinize emerging trends and challenges in the field. This review was guided by insights from Correia et al. [46] and Hamood Alsamhi et al. [47]. Utilizing an analysis matrix, as recommended by Anastasiou et al. [48], this approach systematically organizes and dissects the collected information to uncover patterns and identify underexplored areas, particularly in defensive tactics like data poisoning. The fresh perspectives provided by Cruz González et al. [49] and Marengo et al. [50] have been instrumental in shaping this focus. This method guarantees a concise and structured examination, which is essential for achieving a profound understanding and advancing cybersecurity practices within healthcare environments.

A more thorough review of the literature helped identify gaps in previous studies, offering a strong foundation for the manuscript's contribution. This detailed and organized approach not only provides an in-depth analysis of existing data but also helps generate new insights and strategies. These strategies can be applied to improve cybersecurity defenses against data poisoning in the healthcare sector.

3. Analysis of Results

In this section, the approach is enriched by the inclusion of tables that visually illustrate and support the discussion, with the justification deeply rooted in the works of the cited authors. The increasing interest in the concept of 'data poisoning' within healthcare cybersecurity is highlighted by a substantial body of documented research, underscoring the growing importance of

Table 2
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	150	37.50%
2023	103	25.75%

this defensive strategy. The intersection of 'data poisoning' with 'health' and 'cybersecurity' in academic searches reveals a significant and expanding demand for specialized strategies to mitigate threats in digital health systems (refer to Table 2).

This heightened interest is further corroborated by the contributions of influential scholars such as Palencia-Díaz and de Jesús Palencia-Vizcarra [35], who were among the first to identify the inherent cybersecurity risks within medical environments. Pando's groundbreaking work laid the foundation for further research in this important field. Building on these insights, modern researchers like Kuo and Horn [42] as well as Zerega-Prado and Llerena-Izquierdo [51] have focused on adapting and refining cybersecurity techniques specifically for the healthcare sector. These scholars tackle the evolving challenges posed by digital transformation, offering innovative solutions to protect sensitive medical data.

The tables in this section not only serve as visual aids to simplify complex relationships but also demonstrate the thorough research conducted on the topic. The studies reviewed show that incorporating 'data poisoning' into healthcare cybersecurity strategies is becoming more widely recognized as essential for protecting sensitive medical data. By referencing the work of leading scholars, this section offers a solid rationale for highlighting 'data poisoning' as a critical defense against new cyber threats in digital health systems.

The trend highlighted in Table 2 shows a clear rise in interest among researchers about data poisoning, reflecting how it's becoming a key tool for defending against cyberattacks in the healthcare field. This increase makes it clear that data poisoning is being recognized as a crucial part of strategies to protect sensitive medical information from increasingly sophisticated threats.

Table 3 also showcases a good mix of research methods, including literature reviews, case studies, and hands-on research. This variety shows a well-rounded approach to understanding and applying data poisoning in healthcare cybersecurity. It's not just about studying what's already out there, but also about exploring new ideas and finding better ways to protect patient data.

By blending theoretical research with real-world examples and actual data, the research provides a practical look at how data poisoning is being used and adapted in healthcare environments.

Table 3
Identified scientific studies

Study Type	Articles	Percentage
Literature Review	40	40%
Case Studies	30	30%
Empirical	30	30%

This balanced approach helps ensure that what's learned in theory can be turned into real, effective solutions that stand up to the ever-changing challenges of cybersecurity.

In the end, this thorough look at both established methods and new innovations helps the academic community gain a deeper understanding of how data poisoning can be used to keep healthcare systems safe. This kind of detailed analysis is essential for improving the ways we protect patient information in today's digital and interconnected world, as highlighted in the research findings from Tables 2 and 3.

These findings highlight the crucial need for in-depth research and the development of advanced strategies, like data poisoning, to effectively address the growing cyber threats in the healthcare sector. They point to the urgent requirement for strong regulatory frameworks and stricter data quality controls to improve the security of digital health systems. This aligns with challenges previously noted by Zohuri and McDaniel [52], Zandarín Iragorre [53], as well as Triola [54], who have all emphasized the importance of taking a proactive and informed approach to combat cyberattacks in healthcare settings.

The research begins by examining the escalating complexity of cyberattacks in the healthcare domain, illustrating how tactics like phishing—initially identified by Yarmuch and Barrera [55]—are specifically designed to deceive healthcare staff and gain unauthorized access to confidential information. It then highlights the evolution toward more sophisticated threats, such as malware, which Tian et al. [56] identify as a particularly significant hazard due to its stealthy ability to infiltrate systems undetected.

In response to these challenges, the study explores the urgent need for comprehensive prevention and mitigation strategies. Drawing on Tavera et al. [57], it suggests a multi-pronged approach that combines technical solutions like encryption and two-factor authentication with continuous cybersecurity training for healthcare professionals. The study also emphasizes the need for advanced detection and response systems, along with clear policies for handling cyber incidents, which are essential for building a more resilient cybersecurity framework.

The analysis highlights that the impact of cyberattacks goes far beyond financial losses, seriously threatening patient privacy and confidentiality, which can put their safety and well-being at risk. The study stresses the importance of complying with regulations like the Health Insurance Portability and Accountability Act and the General Data Protection Regulation , which are designed to protect patient rights and ensure the security of health data.

Additionally, the study focuses on the increasing integration of AI in healthcare, emphasizing the need for healthcare professionals to be equipped to handle the new cybersecurity challenges that come with it. Collaboration between different sectors is essential to create a secure healthcare environment where AI can be used safely and effectively. The research also explores the emerging strategy of data poisoning, as highlighted by Maeli and Surwade [58], as a way to protect AI systems in healthcare, underscoring the need for more effective cybersecurity methods in today's increasingly digital world.

Lastly, the study examines the evolving landscape of healthcare cybersecurity, particularly focusing on the roles of data poisoning and AI integration. Experts such as Czekster et al. [59], Kuo and Horn [42], as well as Aljammal et al. [60] emphasize the need to enhance data security in response to emerging threats and highlight the importance of adapting to advanced technologies, such as AI.

Table 4 illustrates the growing interest in AI and cybersecurity in the healthcare sector, reflecting the increasing concerns over data security driven by the rapid pace of digitalization in medicine. This table serves as a visual representation of the need for continued

Table 4
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	5	7.81%

research and the development of strong cybersecurity strategies tailored to the unique challenges of the healthcare industry.

The literature review takes a closer look at how cybersecurity strategies have evolved, with a focus on the growing use of data poisoning as a key tool to protect sensitive health information. Both academics and healthcare professionals are increasingly aware of the need to guard against the more advanced cyberattacks we're seeing today. Recognizing data poisoning as a crucial defense mechanism shows just how serious these threats have become.

What stands out in the review is the emphasis on collaboration across different fields. As Alghawazi et al. [61] mention, bringing together expertise from technology, medicine, and information security is critical to building strong defenses. This type of teamwork ensures that the strategies are not only powerful but also customized to tackle the specific challenges that healthcare faces (see Table 5).

By pooling knowledge from these various areas, this collaborative approach helps to develop solutions that are not only effective but also practical for real-world healthcare settings. The review makes it clear that this kind of multidisciplinary teamwork is essential for dealing with the complex and ever-changing landscape of healthcare cybersecurity. It calls for a coordinated effort to protect patient data and make sure that health information systems remain secure and reliable.

The bubble chart titled *"Panorama of Technological Innovation in Digital Health"* serves an important role in current research. It effectively shows how different technological strategies can help protect patients' digital data from cyber threats. This visual helps to prioritize key research areas, highlighting the contribution each topic makes to improving cybersecurity in the digital health field.

Table 5
Panorama of technological innovation in digital health

Topics	Importance
Data Mining	Medium
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

Note: Since the exact frequency and importance values are not available, terms like 'High,' 'Medium,' and 'Low' are used as placeholders based on their positions in the original graph. These can be updated once specific values are provided.

Data Mining for Security: Ashmore et al. [62] explore how advanced data mining techniques are being used to build early warning systems that protect patient data from unauthorized access, reinforcing the overall cybersecurity setup in healthcare.

IoT and Biomedical Security: Diaz and Gomez [63] look at how IoT is integrated into biomedical devices, focusing on security measures to detect and prevent hacking attempts. This ensures that real-time health data remain secure in today's interconnected healthcare systems.

Strengthening Cybersecurity in Health: Dora et al. [64] dive into advanced cybersecurity techniques that are designed to protect health information from new and emerging threats, safeguarding the confidentiality, integrity, and availability of patient data.

AI for Cyber Defense: Kar et al. [65] discuss how AI can be used to create systems that predict, detect, and stop cyberattacks before they can compromise health data. This is especially important because AI is both a valuable tool and a target in healthcare cybersecurity.

Legislative Support for Data Protection: Liebowitz [66] addresses the need for legal frameworks that not only promote technological innovation but also bolster defenses against cyberattacks, protecting patient privacy in an increasingly digital healthcare landscape.

Machine Learning in Threat Detection: López Julca [67] highlights how machine learning is being applied to analyze patterns in attacks and prevent data breaches. This proactive approach is key to keeping health data safe as threats continue to evolve.

Defense Strategies like Data Poisoning: Kha et al. [68] explore how data poisoning is being used as a defensive strategy, creating traps that confuse and weaken cyber attackers, playing a crucial role in protecting healthcare systems from unauthorized access.

AI in Smart Cities for Health Security: Mengistu et al. [69] examine how AI is used within smart cities to boost the security of health infrastructures, helping detect and respond to security incidents in urban environments. This research emphasizes AI's wider role in protecting not just individual healthcare systems but entire urban health networks.

Countermeasures to Adversarial Attacks in AI: This emerging topic, explored by Mulero-Palencia and Monzon Baeza [70] as well as Rábade-Roca [71], focuses on protecting AI systems in healthcare from adversarial attacks intended to deceive or manipulate them. Ensuring the reliability and safety of AI-based diagnoses and treatments is critical for maintaining trust in these technologies.

Table 6 shows that personal information and medical records are the most common targets in cyberattacks in the healthcare sector. This highlights the urgent need to protect these sensitive data types, especially as healthcare becomes more reliant on AI and other advanced technologies.

This analysis, presented under the theme of *"Healthcare Cybersecurity: Data Poisoning in the Age of AI"*, stresses the growing importance of developing strong and innovative cybersecurity strategies to safeguard sensitive health data. As digitalization and AI integration continue to reshape the healthcare industry, ensuring the security of this data is more critical than ever.

Table 7 shows that phishing is the most commonly used technique in cyberattacks on healthcare systems, followed by malware, MitM attacks, and various social engineering tactics.

Table 6
Most extracted data in cyberattacks on the health sector

Type of data	Percentage
Personal Information	40%
Medical Records	35%
Insurance Information	15%
Payment Data	10%

Table 7
Common tools used in cyberattacks on the health sector

Type of attack	Frequency (%)
Phishing	45%
Malware	30%
Interception (MitM)	15%
Social Engineering	10%

These findings are consistent with the research of Wang et al. [72], underscoring the urgent need to improve current security measures and the importance of comprehensive cybersecurity training for healthcare staff.

Phishing stands out as particularly dangerous because it preys on human error. Even well-trained staff can be tricked into revealing sensitive information through these attacks. This highlights the critical need for stronger awareness programs and specialized training to help staff recognize and stop phishing attempts before they lead to a data breach.

Malware, the second most common threat, is a major concern because it can disrupt healthcare systems and lead to the loss of critical data. To prevent this, healthcare organizations need to have strong antivirus software, keep their systems updated, and monitor their networks regularly to catch malware early and reduce damage.

MitM attacks, which involve secretly intercepting communication between two parties, are especially dangerous in healthcare, where privacy is key. These attacks show how important it is to have secure communication channels and strong encryption to protect sensitive information as it is being transmitted.

Social engineering, where attackers manipulate people into giving away confidential information or doing something that compromises security, further highlights the need for ongoing training. Healthcare staff should be trained to recognize and avoid these types of tricks to help prevent security breaches.

The findings in Table 7 also reflect how cyber threats in healthcare are getting more advanced and varied. As attackers develop new techniques, healthcare systems need to stay ahead by improving not only their technology but also their awareness of cybersecurity risks.

Additionally, there is a clear need for healthcare organizations to invest in better security tools like multi-factor authentication, intrusion detection systems, and AI-driven tools to spot threats early. These solutions help detect and prevent attacks before they can cause serious harm.

In conclusion, Table 7 emphasizes the growing complexity of cyber threats in healthcare and the need for a multi-layered defense strategy. This strategy should include advanced technology, regular staff training, and clear security policies. By taking this approach, healthcare systems can better protect patient data and maintain their operations even as cyber threats continue to evolve.

Table 8 outlines the most common defense strategies that healthcare centers use to protect against cyberattacks, based on studies by Hussmann [4]. The table showcases a wide range of tactics, from advanced methods like data poisoning to more foundational measures such as thorough cybersecurity training, highlighting the variety of tools needed to create a strong defense system.

The research by Hussmann [4] stresses the importance of taking a multi-layered approach to cybersecurity in healthcare settings. One example is data poisoning, an innovative technique that disrupts cyberattacks by feeding attackers misleading or false data, making it difficult for them to access or manipulate sensitive information. As cyber threats continue to grow in complexity, these advanced strategies are becoming more and more critical.

One of the key takeaways is that comprehensive cybersecurity training is crucial because human error is often the weakest link in security systems. By training healthcare staff to recognize and respond to cyber threats, organizations can reduce the risk of breaches caused by mistakes. This training is essential not just for IT staff, but for anyone who handles sensitive information, ensuring everyone is prepared to act as a defense against attacks.

Table 8 also highlights other important strategies, such as multi-factor authentication, encryption, and regular security audits. Multi-factor authentication provides an extra layer of security by requiring multiple steps to verify a user's identity, making it harder for unauthorized users to gain access. Encryption protects data both when it's stored and while it's being transmitted, ensuring that even if the data is intercepted, it remains unreadable. Regular security audits help identify weaknesses in the system and allow organizations to fix them before cybercriminals can exploit them.

The research by Hussmann [4] makes it clear that a well-rounded cybersecurity strategy is necessary, one that combines various tools and methods into a single, cohesive plan. No single solution is enough to protect healthcare systems from the wide variety of threats they face today. It takes a combination of advanced technology, proper training, and ongoing risk

Table 8
Main defenses 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 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

assessments to create a security system that can stand up to the growing threats in the digital world.

Additionally, the findings in Table 8 highlight how important it is for cybersecurity strategies to stay flexible and adaptable. As cyber threats evolve, so must the defenses used to counter them. This forward-thinking approach helps ensure healthcare systems are always one step ahead, protecting both the integrity of their operations and the privacy of their patients.

In conclusion, Table 8 provides a solid overview of the most effective strategies healthcare organizations can use to guard against cyberattacks. By adopting a multi-layered approach, as suggested by Hussmann [4], healthcare providers can build a robust cybersecurity framework that is equipped to handle the challenges of today's digital landscape.

4. Discussion

It is clear that healthcare needs to move beyond current security practices and adopt more advanced methods to prevent cyberattacks. As Kuo and Horn [42] as well as Salmi and Bogucka [23] point out, the growing complexity of threats requires a more sophisticated approach. This study highlights the importance of paying close attention to cybersecurity, especially with the increasing use of AI in healthcare. Techniques like data poisoning are becoming essential tools to throw off attackers and protect patient information. These methods are a big improvement over older security measures, which often fall short when facing today's more advanced threats.

A deeper comparison with existing literature reveals that while previous studies have acknowledged the importance of enhancing threat detection capabilities, they have not fully explored the potential of data poisoning as a proactive defense mechanism. For instance, Bernstam et al. [10] and Medina-Arco et al. [11] emphasize the prevention of identity theft and unauthorized information extraction but do not delve into the strategic deployment of data poisoning within AI systems. This study, therefore, contributes uniquely by integrating these advanced methods into the broader framework of cybersecurity strategies tailored for the healthcare sector.

The analysis highlights the urgent need to not only develop advanced technologies but also to implement strong methods for addressing the increasing complexity of cyber threats. As noted by Giambelluca [18] as well as Kuo and Horn [42], it is crucial to create a regulatory framework specifically designed for AI in healthcare to ensure both security and ethical standards. This approach shows how security practices must evolve alongside technology to tackle the unique challenges at the intersection of AI and healthcare.

In addition, the insights from Brilhante et al. [19] and Medina-Arco et al. [11] provide valuable perspectives on current strategies aimed at strengthening data security in medical AI. Their research focuses on key concerns like preventing identity theft and unauthorized data access, which are critical issues as healthcare continues to digitalize. These strategies aim to create a secure and trustworthy clinical environment despite the growing sophistication of cyber threats. This study builds on their work by proposing the use of data poisoning as an extra layer of protection, adding to a more resilient cybersecurity framework.

Maintaining a strong digital infrastructure capable of defending against attacks while protecting sensitive health data is another key takeaway from this study. This aligns with existing research, which consistently emphasizes the importance of advanced security practices that address the specific challenges posed by AI in healthcare. By comparing these findings with previous studies, it becomes clear that adopting more sophisticated strategies, such as data poisoning, is essential for protecting the future of healthcare in an increasingly digital world.

In conclusion, this study emphasizes the need for current security practices to adapt to rapid technological advancements and the growing complexity of cyber threats. Adding data poisoning to cybersecurity strategies, along with developing strong regulatory frameworks, offers a way for healthcare systems to better protect patient information and ensure the reliability of AI-driven medical environments. This research not only contributes to the theoretical understanding of these issues but also provides practical recommendations for improving cybersecurity in healthcare, addressing a significant gap in current literature.

5. Conclusion and Policy Recommendations

This study highlights the growing importance of data poisoning as a key element in cybersecurity strategies within healthcare information systems, especially as these systems become more digitalized. The increasing integration of AI in healthcare is not only transforming traditional practices but also strengthening the sector's defenses against a wide range of cyber threats.

When used correctly, data poisoning serves as a proactive tool to protect patient information. By introducing false data in response to malicious activity, this technique makes it harder for attackers to access sensitive information. As cyberattacks become more sophisticated, this kind of advanced defense is becoming essential.

The study makes several important contributions to healthcare cybersecurity. First, it demonstrates how data poisoning can be used not just as a defense mechanism but as part of a broader strategy that integrates smoothly with AI-powered systems. This highlights AI's dual role: it both enhances healthcare and becomes a target for cyberattacks.

Second, the study explains how data poisoning can be implemented in real-world healthcare settings without disrupting operations. This balance between security and functionality is crucial, especially in healthcare, where smooth operations are key.

Third, the research stresses the importance of collaboration between AI experts, cybersecurity professionals, and healthcare workers. This teamwork is critical for ensuring that advanced cybersecurity measures like data poisoning are applied effectively and ethically.

However, the study also acknowledges some limitations. The main limitation is the need for more real-world testing. While the theory behind data poisoning is well-established, its practical application in various healthcare environments requires further validation. There may be challenges that were not anticipated in theory, particularly in terms of how it impacts day-to-day healthcare operations.

Another limitation involves ethical concerns. Introducing false data, even for security purposes, raises questions about the ethical boundaries of such practices. While this study touches on these issues, it calls for a more in-depth ethical analysis to ensure that the use of data poisoning aligns with the highest standards of patient care and data protection.

The study also opens several areas for future research. One important direction is developing more accurate detection methods to determine when and where data poisoning should be applied. As AI continues to evolve, so too must the strategies that protect it from manipulation. Future research should explore how newer AI technologies, such as reinforcement learning and generative models, interact with data poisoning techniques.

Another area to explore is the long-term impact of data poisoning on healthcare systems—not only the immediate security benefits but also how it affects data integrity, system performance,

and patient care outcomes. Long-term studies would provide valuable insights into the sustainability of these strategies.

Finally, applying data poisoning beyond healthcare to sectors like finance and infrastructure could uncover its broader implications for cybersecurity across industries. As the digital landscape becomes more interconnected, the lessons learned from healthcare cybersecurity could inform strategies in other sectors facing similar challenges.

In conclusion, the adoption of data poisoning represents a significant advancement in protecting healthcare information systems from a wide range of cyber threats. By incorporating this strategy, healthcare organizations can improve their defenses, safeguard patient data, and strengthen the overall security of their systems. However, as healthcare continues to evolve in the digital age, cybersecurity practices, including data poisoning, must adapt to keep pace with increasingly complex cyber threats.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by the author.

Conflicts of Interest

The author declares that he has no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Edwin Gerardo Acuña Acuña: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration, Funding acquisition.

References

[1] 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

[2] Acuña, E. G. A. (2023). Data mining and internet of things (IoT) application for biomedical products. *Techno Review. International Technology, Science and Society Review*, *13*(1), 145–169. https://doi.org/10.37467/revtechno.v12.3444

[3] López-Aguilar, P., Batista, E., Martínez-Ballesté, A., & Solanas, A. (2022). Information security and privacy in railway transportation: A systematic review. *Sensors*, *22*(20), 7698. https://doi.org/10.3390/s22207698

[4] Hussmann, K. (2020). Corrupción en el sector salud. *Recomendaciones Prácticas Para Donantes*, *16*(U4 Issue), 45–62.

[5] Gil Membrado, C. (2021). *E-salud, autonomía y datos clínicos: Un nuevo paradigma. e-salud, autonomía y datos clínicos*. Spain: Dykinson.

[6] 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

[7] 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

[8] Hathaliya, J. J., Tanwar, S., & Sharma, P. (2022). Adversarial learning techniques for security and privacy preservation: A comprehensive review. *Security and Privacy*, *5*(3), e209. https://doi.org/10.1002/spy2.209

[9] 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

[10] Bernstam, E. V., Shireman, P. K., Meric, B. F., Zozus, M. N., Jiang, X., Brimhall, B. B., ..., & Becich, M. J. (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

[11] 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

[12] Matsuzaka, Y., & Yashiro, R. (2023). AI-based computer vision techniques and expert systems. *AI*, *4*(1), 289–302. https://doi.org/10.3390/ai4010013

[13] 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

[14] Cirio, J. J., Diluca, P., Ciardi, C., Scrivano, E., Lundquist, J., Lylyk, I. R., ..., & Lylyk, P. (2023). Impact of artificial intelligence on therapeutic metrics of cerebrovascular attack during the COVID-19 pandemic. *Medicina*, *83*(5), 705–718.

[15] Sabouri, E., Saburi, A., Gerami, R., Zeraati, T., Saburi, E., & Ghanei, M. (2023). Computerized intelligence and mathematical models for COVID-19 diagnosis: A review. *Journal of Human Environment & Health Promotion*, *9*(2), 55–62. https://doi.org/10.61186/jhehp.9.2.55

[16] Rugo, A., Ardagna, C. A., & El Ioini, N. (2023). A security review in the UAVNet era: Threats, countermeasures, and gap analysis. *ACM Computing Surveys*, *55*(1), 1–35. https://doi.org/10.1145/3485272

[17] Ayma Quirita, V. H., Achanccaray Díaz, P. M., Arauco Canchumuni, S. W., & Soto Vega, P. J. (2022). Desafíos del aprendizaje profundo en la visión por computador. In *Actas del V Congreso Internacional de Ingeniería de Sistemas*, 49–53. https://doi.org/10.26439/ciis2022.6070

[18] Giambelluca, F. L. (2022). *Detección automática, clasificación y reconocimiento de escorpiones mediante técnicas de aprendizaje profundo*. PhD Thesis, Universidad Nacional de La Plata.

[19] Brilhante, D. da S., Manjarres, J. C., Moreira, R., de Oliveira Veiga, L., de Rezende, J. F., Müller, F., ..., & de Figueiredo, F. A. P. (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

[20] Gómez-de-Ágreda, Á., Feijóo, C., & 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

[21] Akhtar, P., Ghouri, A. M., Khan, H. U. R., Amin ul Haq, M., Awan, U., ..., & Ashraf, A. (2023). Detecting fake news and

disinformation using artificial intelligence and machine learning to avoid supply chain disruptions. *Annals of Operations Research*, *327*(2), 633–657. https://doi.org/10.1007/s10479-022-05015-5

[22] Sánchez, B. C. C., & Rojas, C. A. O. (2022). Análisis de seguridad entre microservicios con Amazon web service. *Revista Logos Ciencia & Tecnologia*, *14*(2), 42–52. https://doi.org/10.22335/rlct.v14i2.1546

[23] Salmi, Y., & Bogucka, H. (2024). Poisoning attacks against communication and computing task classification and detection techniques. *Sensors*, *24*(2), 338. https://doi.org/10.3390/s24020338

[24] Rojas Buenaño, A. I. (2021). *Sistema de monitoreo y detección de defacements en sitios web. Un enfoque moderno*. Master's Thesis. Pontificia Universidad Católica del Ecuador.

[25] Saini, S., & Saxena, N. (2023). A survey of threats to research literature-dependent medical AI solutions. *ACM Computing Surveys*, *55*(14s), 1–26. https://doi.org/10.1145/3592597

[26] Das, D., Sharma, U., & Bhattacharyya, D. K. (2019). Defeating SQL injection attack in authentication security: An experimental study. *International Journal of Information Security*, *18*(1), 1–22. https://doi.org/10.1007/s10207-017-0393-x

[27] Li, B., Qi, P., Liu, B., Di, S., Liu, J., Pei, J., . . . , & Zhou, B. (2023). Trustworthy AI: From principles to practices. *ACM Computing Surveys*, *55*(9), 1–46. https://doi.org/10.1145/3555803

[28] Acuña, E. G. A. (2022). Analysis of the impact of TIC on higher education in Latin America. *Edutech Review. International Education Technologies Review*, *9*(1), 15–29. https://edulab.es/revEDUTECH/article/view/3277

[29] Marin, G. H., Cañas, M., Marin, G., Marin, L., Nucher, D., Diaz Pérez, D., & Urtasun, M. (2023). Impacto económico de medicamentos de alto precio/costo en la seguridad social de Argentina. El caso del instituto de obra social para las Fuerzas Armadas y de seguridad. *Medicina (Buenos Aires)*, *83*(1), 65–73. https://doi.org/10.1016/j.medici.2023.01.003

[30] Singh, A., Satapathy, S. C., Roy, A., & Gutub, A. (2022). AI-based mobile edge computing for IoT: Applications, challenges, and future scope. *Arabian Journal for Science & Engineering*, *47*(8), 9801–9831. https://doi.org/10.1007/s13369-021-06348-2

[31] Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, *15*(18), 6799. https://doi.org/10.3390/en15186799

[32] Roldán Álvarez, M. Á., & Vargas Montoya, H. F. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. *Ingeniería y Desarrollo*, *38*(2), 279–297. https://doi.org/10.14482/inde.38.2.006.31

[33] Qahri-Saremi, H., & Turel, O. (2023). Situational contingencies in susceptibility of social media to phishing: A temptation and restraint model. *Journal of Management Information Systems*, *40*(2), 503–540. https://doi.org/10.1080/07421222.2023.2196779

[34] Sheehan, A. E., Bounoua, N., Rose, R. E., Sadeh, N., & Javdani, S. (2024). Profiles of risk for self-injurious thoughts and behaviors among system-impacted girls of color. *Journal of the American Academy of Child & Adolescent Psychiatry*, *63*(9), 898–907.

[35] Palencia-Díaz, R., & de Jesús Palencia-Vizcarra, R. (2023). El potencial de la inteligencia artificial para disminuir errores médicos y mejorar la educación médica continua. *Medicina Interna de Mexico*, *39*(3), 419–421. https://doi.org/10.24245/mim.v39i3.8934

[36] Sarajchi, M., & Sirlantzis, K. (2023). Diseño y control de un exoesqueleto de una sola pierna con compensación de gravedad para niños con parálisis cerebral unilateral. *Sensors*, *23*(13), 6103. https://doi.org/10.3390/s23136103

[37] Mora Pineda, J. (2022). Modelos predictivos en salud basados en aprendizaje de maquina (machine learning). *Revista Médica Clínica Las Condes*, *33*(6), 583–590. https://doi.org/10.1016/j.rmclc.2022.11.002

[38] Francisco Ávila-Tomás, J., Olano-Espinosa, E., Minué-Lorenzo, C., Javier Martínez-Suberbiola, F., Matilla-Pardo, B., & Serrano-Serrano, E. (2019). Nuevas herramientas de comunicación digitales entre profesionales de la salud y pacientes. A propósito del proyecto Dejal@Bot. *Revista de Comunicación y Salud*, *9*(2), 55–70. https://doi.org/10.35669/revistadecomunicacionysalud.2019.9(2).55-70

[39] Nappa, A., Úbeda-Portugués, A., Papadopoulos, P., Varvello, M., Tapiador, J., & Lanzi, A. (2022). Scramblesuit: An effective timing side-channels framework for malware sandbox evasion. *Journal of Computer Security*, *30*(6), 851–876. https://doi.org/10.3233/JCS-220005

[40] Munkøe, M., & Mölder, H. (2022). La ciberseguridad en la era de hipercompetitividad: ¿Puede la UE afrontar los nuevos retos? *Revista CIDOB d'Afers Internacionals*, *131*, 69–94. https://doi.org/10.24241/rcai.2022.131.2.69

[41] Parra, L., Marin Peira, J. F., Lloret, A. T., & Lloret, J. (2024). Evaluating the impact of natural products to improve the sustainability or urban lawns. *Cities*, *150*, 105097. https://doi.org/10.1016/j.cities.2024.105097

[42] 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 (TOCHI)*, *30*(6), 1–37. https://doi.org/10.1145/3609325

[43] Zare, S., Meidani, Z., Ouhadian, M., Akbari, H., Zand, F., Fakharian, E., & Sharifian, R. (2022). Identification of data elements for blood gas analysis dataset: A base for developing registries and artificial intelligence-based systems. *BMC Health Services Research*, *22*(1), 317. https://doi.org/10.1186/s12913-022-07706-y

[44] Muñoz-del-Carpio-Toia, A., Mondragón-Barrios, L., Duro, E. A., Castro, L. R., & Sorokin, P. (2023). Protección de datos de salud: El reto de la armonización legislativa en América Latina. *Revista del Cuerpo Médico del Hospital Nacional Almanzor Aguinaga Asenjo*, *16*(2), 1–13.

[45] Shalev-Shwartz, S., & Ben-David, S. (2014). *Understanding machine learning: From theory to algorithms*. UK: Cambridge University Press.

[46] Correia, M., Rego, G., & Nunes, R. (2021). The right to be forgotten and COVID-19: Privacy versus public interest. *Acta Bioéthica*, *27*(1), 59–67. https://doi.org/10.4067/s1726-569x2021000100059

[47] Hamood Alsamhi, S., Hawbani, A., Shvetsov, A. V., & Kumar, S. (2023). Advancing pandemic preparedness in healthcare 5.0: A survey of federated learning applications. *Advances in Human-Computer Interaction*, *2023*(1), 9992393. https://doi.org/10.1155/2023/9992393

[48] Anastasiou, T., Karagiorgou, S., Petrou, P., Papamartzivanos, D., Giannetsos, T., Tsirigotaki, G., & Keizer, J. (2022). Towards robustifying image classifiers against the perils of adversarial attacks on artificial intelligence systems. *Sensors*, *22*(18), 6905. https://doi.org/10.3390/s22186905

[49] Cruz González, J. P., Castiblanco Jiménez, I. A., Martínez Caicedo, S., Galvis Sabogal, L. A., & Gómez Acevedo, J. S. (2022). Identificación de la correcta disposición de desperdicios generados por COVID-19 en Colombia aplicando systemic design. *Producción + Limpia*, *17*(2), 134–153. https://doi.org/10.22507/pml.v17n2a8

[50] Marengo, L. L., Martinez Kozyreff, A., da Silva Moraes, F., Gomes Maricato, L. I., & Barberato-Filho, S. (2022). Tecnologias móviles en salud: Reflexiones sobre desarrollo, aplicaciones, legislación e ética. *Revista Panamericana de Salud Pública*, *46*, e37. https://doi.org/10.26633/RPSP.2022.37

[51] Zerega-Prado, J., & Llerena-Izquierdo, J. (2022). Arquitectura de consolidación de la información para seguros de la salud mediante big data. *Memoria Investigaciones en Ingeniería*, *23*, 18–31. https://doi.org/10.36561/ING.23.3

[52] Zohuri, B., & McDaniel, P. (2022). Global suicide rate among youngsters increasing significantly. In *Transcranial Magnetic and Electrical Brain Stimulation for Neurological Disorders,* 343–355. https://doi.org/10.1016/b978-0-323-95416-7.00007-9

[53] Zandarín Iragorre, M. T. (2021). Normativa, gestión de riegos y experiencia sobre depósitos de relaves en Chile. *Boletin Geologico y Minero*, *132*(4), 573–581. https://doi.org/10.21701/bolgeomin.132.4.012

[54] Triola, M. F. (2004). *Probabilidad y estadística*. USA: Pearson Educación.

[55] Yarmuch J., & Barrera A. (2024). Tomo de resumenes del 95 congreso Chileno e internacional de cirugía. *Revista de Cirugía*, *76*(1), 1–20. http://dx.doi.org/10.35687/s2452-454920230011712

[56] Tian, L., Shang, F., & Gan, C. (2023). Optimal control analysis of malware propagation in cloud environments. *Mathematical Biosciences and Engineering*, *20*(8), 14502–14517. https://doi.org/10.3934/mbe.2023649

[57] Tavera, E., Gamarra Ruiz, M. M., Alatrista, R., & Vásquez Pacheco, V. (2023). Representaciones sociales sobre la experiencia de elaborar pósteres académicos: el caso de estudiantes de Ingeniería Electrónica en un curso de escritura. *Pensamiento Educativo*, *60*(3), 1–15. https://doi.org/10.7764/PEL.60.3.2023.8

[58] Maeli, S. A. A. O., & Surwade, A. U. (2023). Phishing e-mail detection and blocking it based on the header elements. *Grenze International Journal of Engineering & Technology*, *9*(2), 248–252.

[59] Czekster, R. M., Grace, P., Marcon, C., Hessel, F., & Cazella, S. C. (2023). Challenges and opportunities for conducting dynamic risk assessments in medical IoT. *Applied Sciences*, *13*(13), 7406. https://doi.org/10.3390/app13137406

[60] Aljammal, A. H., Taamneh, S., Qawasmeh, A., & Salameh, H. B. (2023). Machine learning based phishing attacks detection using multiple datasets. *International Journal of Interactive Mobile Technologies*, *17*(5), 71–83. https://doi.org/10.3991/ijim.v17i05.37575

[61] Alghawazi, M., Alghazzawi, D., & Alarifi, S. (2023). Deep learning architecture for detecting SQL injection attacks based on RNN autoencoder model. *Mathematics*, *11*(15), 3286. https://doi.org/10.3390/math11153286

[62] Ashmore, R., Calinescu, R., & Paterson, C. (2022). Assuring the machine learning lifecycle: Desiderata, methods, and challenges. *ACM Computing Surveys*, *54*(5), 1–39. https://doi.org/10.1145/3453444

[63] Diaz, J., & Gomez, S. (2023). Tecnologías y educación, una relación ética. *Question*, *3*(76), e851. https://doi.org/10.24215/16696581e851

[64] Dora, J. R., Hluchý, L., & Nemoga, K. (2023). Ontology for blind SQL injection. *Computing and Informatics*, *42*(2), 480–500. https://doi.org/10.31577/cai_2023_2_480

[65] Kar, D., Panigrahi, S., & Sundararajan, S. (2016). SQLiDDS: SQL injection detection using document similarity measure. *Journal of Computer Security*, *24*(4), 507–539. https://doi.org/10.3233/JCS-160554

[66] Liebowitz, J. (2020). *Data analytics and AI*. USA: CRC Press.

[67] López Julca, R. R. (2023). *Teoría de la imputación objetiva y autoría mediata del programador de inteligencia artificial para fines delictivos en el Perú*. PhD Thesis, Universidad Nacional Santiago Antúnez de Mayolo.

[68] Kha, Q.-H., Le, V.-H., Hung, T. N. K., Nguyen, N. T. K., & Le, N. Q. K. (2023). Development and validation of an explainable machine learning-based prediction model for drug–food interactions from chemical structures. *Sensors*, *23*(8), 3962. https://doi.org/10.3390/s23083962

[69] Mengistu, T. M., Kim, T., & Lin, J.-W. (2024). A survey on heterogeneity taxonomy, security and privacy preservation in the integration of IoT, wireless sensor networks and federated learning. *Sensors*, *24*(3), 968. https://doi.org/10.3390/s24030968

[70] Mulero-Palencia, S., & Monzon Baeza, V. (2023). Detection of vulnerabilities in smart buildings using the shodan tool. *Electronics*, *12*(23), 4815. https://doi.org/10.3390/electronics12234815

[71] Rábade-Roca, J. (2018). La innovación policial en la ciudad del siglo XXI. In *6 Conference Creatives Cities*. https://doi.org/10.7195/piccc.00040

[72] Wang, Y. C., Zhang, G. L., & Zhang, Y. L. (2023). Analysis of SQL injection based on petri net in wireless network. *Journal of Information Science & Engineering*, *39*(1), 167–181. https://doi.org/10.6688/JISE.202301_39(1).0010

How to Cite: 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