Review

Data Security in AI Healthcare Applications: Challenges and Innovative Methods

Aleksandar Stankovic * and Marina Marjanovic

Posted Date: 9 July 2025

doi: 10.20944/preprints202507.0821.v1

Keywords: healthcare security; Industry 4.0; blockchain; honeypots; zero-knowledge proofs; adversarial attacks; cybersecurity; data security and integrity

Article

Data Security in AI Healthcare Applications: Challenges and Innovative Methods

Aleksandar Stankovic *,† **and Marina Marjanovic**

Singidunum University
* Correspondence: aleksandar.stankovic.23@singimail.rs
† Current address: Belgrade, Serbia.

Abstract

Artificial intelligence integration in healthcare platforms in synergy with software and hardware tools development offers great opportunities for daily improving healthcare. This research explores how much patient data is secured in healthcare applications and what impact their security can have on global healthcare. Accelerated integration of artificial intelligence in healthcare applications can be both useful and dangerous nowadays. Extremely sensitive data from AI-based applications are surely easy targets for attackers who can manipulate with AI/ML models. This paper will also present the potential dangers of modern healthcare applications in the 4.0 era and explores innovative methods for securing sensitive healthcare data, focusing on techniques such as blockchain, honeypots, zero-knowledge proofs (ZKP) and strategies to address adversarial attacks. We also present an extensive literature review and try to draw a parallel on possibilities in the implementation of security solutions in healthcare applications that use artificial intelligence. Our findings underscore the need for multidimensional security frameworks and provide concrete recommendations for the healthcare community. Ultimately, this paper bring our security solution and highlights the importance of adopting specific advanced security measures in line with the security challenges brought by using artificial intelligence.

Keywords: healthcare security; Industry 4.0; blockchain; honeypots; zero-knowledge proofs; adversarial attacks; cybersecurity; data security and integrity

1. Introduction

In recent years, the landscape of healthcare data security continues to evolve at an alarming pace, presenting an array of challenges for both healthcare management and security specialists. Recent investigations have revealed a noticeable rise in the frequency and severity of data breaches, with many incidents attributed to sophisticated hacking techniques and unauthorized access. In 2024, 275,000,000 individuals were affected by healthcare security breaches. These breaches, which compromise millions of patient data records over the world, underscore the increasingly critical need for robust cybersecurity measures across healthcare organizations. As healthcare records become prime targets for malicious actors due to valuable patients medical and personal information, the urgency to address these vulnerabilities is very important. This study examines the attack vectors, mitigation techniques and author conclusions to provide a comprehensive understanding of AI's role and risks in healthcare. In particular, it focuses on advanced techniques such as blockchain, zero-knowledge proofs, honeypots and other dynamic defense strategies targeting adversarial attacks. The review synthesizes papers and findings on this specific topic and tries to break down the attacks on artificial intelligence models used in healthcare applications to bring closer the direction in which future research should move. We will present, in our opinion, defense techniques that in the future could best be adapted to defense against data attacks in healthcare, given the sensitivity of the data being handled. As primary defense techniques, we will present works that use blockchain, ZKP and honeypot and give a proposal for future research at the end of the paper. Blockchain technology has been pointed out as a robust solution for enhancing the security and transparency of AI systems in healthcare. By leveraging its decentralized and immutable nature, blockchain can address several vulnerabilities associated with adversarial attacks. Blockchain operates by maintaining a distributed ledger of transactions, ensuring data integrity and traceability. In the context of healthcare AI, blockchain can be used to secure medical data, verify model integrity, and ensure the origin of AI decisions. For instance, blockchain can be employed to track the origin of medical data sets used for training AI models, preventing data poisoning attacks where adversaries manipulate training data to compromise model performance [1]. Zero-knowledge proofs (ZKP) are cryptographic techniques that enable one party to prove the validity of a statement without revealing any underlying information to each other. This concept has been applied to AI security, offering a novel approach to defending against adversarial attacks. Zero-knowledge proofs can be integrated into AI systems to ensure the confidentiality of sensitive data while maintaining model accuracy. In healthcare, ZKPs can be used to verify the integrity of AI predictions without exposing patient data or model parameters. This is particularly useful in scenarios where data privacy is very important, such as in medical diagnosis systems [2]. Last, but not least, is Honeypots that represents decoy systems or data designed to attract and detect malicious actors. In the context of AI security, honeypots can be used to identify and analyze adversarial attacks, providing valuable insights for defense strategies. Honeypots can be deployed in healthcare AI systems to force adversaries into revealing their attack methods and techniques. For example, a high-interaction honeypot (HIHP) can mimic a real AI model, allowing researchers to study adversarial tactics and develop countermeasures. Additionally, honeypots can be used to detect data poisoning attacks by identifying anomalies in input patterns [3].

2. Review

This paper includes an overview of scientific research on data security in healthcare applications that use AI. Also, the focus will be on mitigation techniques and conclusions at which level the scientific community has currently managed to establish some principles of defense against attacks on AI models. To conduct this review, we analyze existing research papers in this field. We identified the main attack vectors, mitigation techniques, also we share author conclusion for easier comparing dangerous attacks in healthcare applications. For the defense technique, we chose blockchain, ZKP and honeypot, which in our opinion are the future of defense against attacks on healthcare applications that use AI. The methodology followed next rules: to collect the different works, the main scientific databases and publishers (MDPI, Springer, arXiv, IEEE, Google Scholar). Were inspected mainly newer works (to get the latest information) and using different keywords relevant for attacks on data in healthcare applications (poison attack, adversarial attacks, network anomalies, data breaches, deepfake attacks). Papers we analyze focused on hybrid security frameworks that integrate multiple advanced security techniques as we can see on Figure 1. For instance, a multi-layered approach combining blockchain with ZKP has been posited to deliver more comprehensive protection, addressing both data integrity and confidentiality threats simultaneously. The real-world implications of these security challenges have been highlighted in several research papers.

doi:10.20944/preprints202507.0821.v1

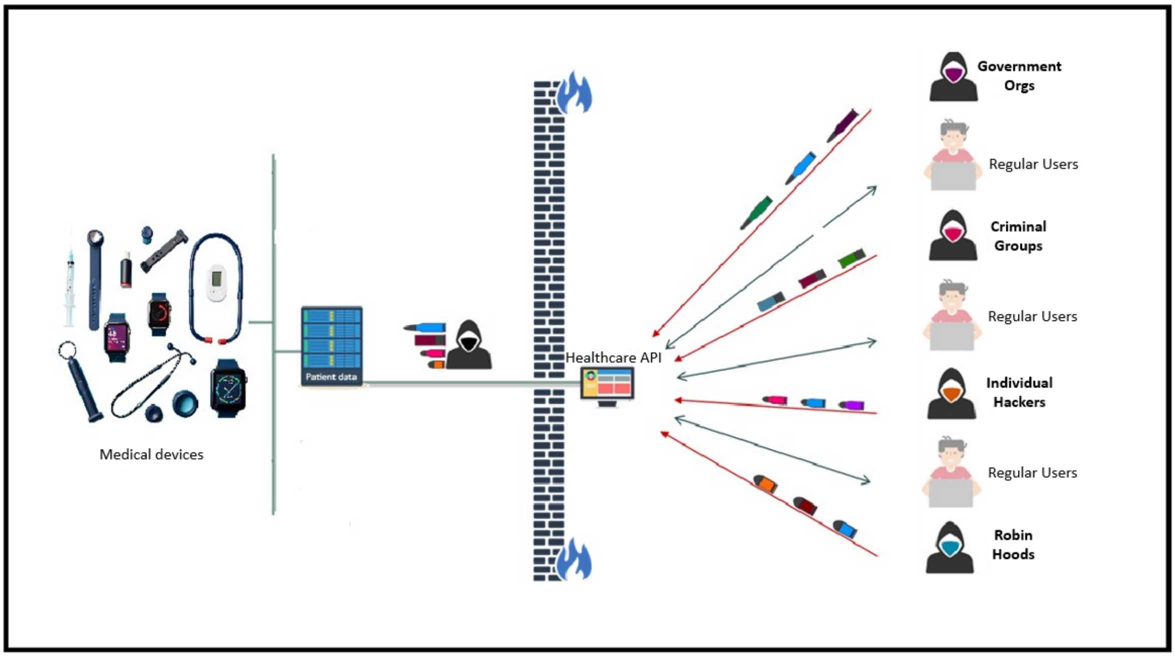

Figure 1. Hackers and regular users of healthcare applications.

Table 1 provides a synthesized overview of latest research papers reviewed in this study, capturing their publication details, attack vectors, mitigation technique and author conclusion. The surveyed literature reveals that innovative security methodologies, while promising, face challenges in real-world applications due to system complexity, resource constraints, and evolving adversarial tactics. Advanced cryptographic techniques like zero-knowledge proofs offer strong confidentiality without revealing sensitive data. However, their integration into existing healthcare infrastructure is often slow down by computational demands and latency [2]. Similarly, blockchain's benefits in healthcare, such as transparency and immutability, are offset by scalability and interoperability limitations [1,4]. The complex management of multiple advanced systems require a thorough cost-benefit analysis for practical deployment. On the other side, honeypots are effective in detecting and analysing cyberattacks, provide valuable real-time insights into attacker behaviour. Artificial intelligence integration has improved threat identification within honeypot systems. Yet, high false positive rates and the intensive requirements of continuous data monitoring produce ongoing challenges. A prominent trend highlights the necessity for adaptive hybrid security architectures capable of addressing multiple vulnerabilities simultaneously. The synergy combination of blockchain, zero-knowledge proofs, and honeypots shows potential in future data security [3].

Table 1. This is a wide table.

Publication details	Attack vectors	Mitigation technique	Author conclusion
Strengthening Healthcare Data Security with AI-Powered Threat Detection [5]	Cyber threats, network anomalies	AI-driven solutions (ML, anomaly detection), continuous network monitoring, predictive analytics	AI enables proactive identification of cyber threats, automated incident response, and enhanced data security.
Healthcare Cybersecurity: Data Poisoning in the Age of AI [6]	Data poisoning	Innovative solutions to protect patients and institutions	Highlights security protocol weaknesses and the urgent need for innovative solutions.
AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity [7]	Cybercriminals targeting electronic health records, telemedicine, and mobile health apps	AI in healthcare data security	AI is a significant development for securing patient information in the face of increasing cyber threats.
Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review [4]	Data breaches, lack of data privacy	Blockchain for secure EHR management, patient identity management, and secure data transmission; AI for clinical analysis and prediction	The fusion of blockchain and AI can address critical challenges in securing EHRs, ensuring data privacy, and facilitating secure data transmission.
Artificial Intelligence Security: Threats and Countermeasures [8]	Data poisoning, adversarial attacks, data breaches, AI bias	Detection & Filtering, Data Provenance & Standardized Logging, ROBN, Homomorphic encryption, E2E differential privacy, Model watermarking, Learning fair models, Bias diagnostic	AI-based systems are vulnerable to various security threats throughout the whole process, ranging from data collection to training, inference, and final deployment.
A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare [9]	Malicious activities, damaging attacks, unauthorized access	Enhanced security protocols, monitoring tools, intrusion detection systems	Cybersecurity in healthcare is critical due to the sensitive nature of patient data and the increasing sophistication of cyberattacks.
healthAIChain: Improving security and safety using Blockchain Technology applications in AI-based healthcare systems [10]	Threats to online data, medical and patient data	Blockchain technology	Blockchain can promote highly configurable openness while retaining the highest levels of security.
Artificial Intelligence in Healthcare: Safeguarding Data and Enhancing Information Access through Cybersecurity [11]	Emerging cyber threats	AI for risk prediction, vulnerability detection, cryptography, compliance with essential security requirements, blockchain	AI can proactively predict risks and block chain enhances data integrity.
Cybersecurity in the AI Era Measures Deepfake Threats and Artificial Intelligence-Based Attacks [12]	Deepfake attacks and AI-based cyberattacks	Enhanced security protocols	Deepfake technology enables video and audio manipulation with a high level of realism, which can be used for disinformation, fraud, and threats to digital security systems.
Securing AI-based Healthcare Systems using Blockchain Technology: A State-of-the-Art Systematic Literature Review and Future Research Directions [13]	Lack of medical datasets for training AI models, adversarial attacks, and a lack of trust due to its black box working style	Blockchain technology	Blockchain technology can improve the reliability and trustworthiness of AI-based healthcare.

Arefin [7] highlighted a comprehensive analysis of the AI role in enhancing cybersecurity within the healthcare sector. The implementation of digital solutions increasingly requires the application of secure and serious security solutions, particularly given the sensitive nature of healthcare data. In this work, the authors highlight how machine learning and anomaly detection, artificial intelligence technologies, can proactively identify and mitigate cyber threats and ensure information security and regulatory compliance. The advantage of this work is the detailed investigation of various artificial intelligence methodologies, which are key to detecting anomalies and predicting potential vulnerabilities in healthcare applications. The most important methods are supervised learning, unsupervised and semi-supervised learning. Crucial for minimizing the impact of data breaches and maintaining operational continuity the importance of AI provided real-time incident response facilitated by AI. They also did not leave out ethical considerations in terms of the need for truly unbiased and transparent algorithms and the need for robust technological solutions. This paper provides a good overview of the potential and the need for further steps in the application of cybersecurity in healthcare. It is excellent for researchers and practitioners because it provides valuable insights into the transformative

doi:10.20944/preprints202507.0821.v1

potential of artificial intelligence in healthcare cybersecurity, while also highlighting the ethical and operational challenges that must be overcome. It also highlights the importance of a collective effort, i.e. collaboration between healthcare professionals, technology companies, and regulatory bodies, to adequately harness the potential of AI for the betterment of all.

Gerardo [6] focuses on weaknesses in existing security protocols and vulnerabilities specific to healthcare software. It highlights cybersecurity challenges in this area and highlights data poisoning threats as the most important ones to pay attention to due to increasing digitalization. Weaknesses in security mechanisms are clearly identified that can allow potential attackers to compromise sensitive information and undermine the effectiveness of digital tools. He also proposes advanced cybersecurity strategies such as multi-layered attack detection and mitigation systems. By presenting real-world examples and research, author demonstrate the broader impact on business processes of how these challenges can hinder the necessary digital transformation in modern healthcare services. The conclusion of this study is that joint actions are needed by regulators and developers to develop new security technologies and implement strict regulations to protect data integrity and ensure a secure digital transition.

Arefin et al. [5] discusses AI-based solutions for healthcare data protection and cybersecurity innovations and their significance. The potential for exposing patients' private data to cybercrime is noted. This relates to the digitalization of healthcare, specifically technologies such as electronic health records, telemedicine, and mobile health applications that have improved patient care and operational efficiency but have also compromised their data. Advanced threats such as ransomware and phishing require much more advanced cybersecurity measures. The paper focuses on the advantages and challenges, with the advantages being AI technology's real-time response, fast and efficient analysis of huge amounts of data, advanced encryption, and data anonymity. However, the challenges include concerns about patient privacy, possible algorithm bias, high integration costs, and the vulnerability of AI algorithms to attacks. They cite next-generation technologies such as federated learning, quantum-resistant encryption, and AI-based threat intelligence sharing as potential solutions. The conclusion from this research is that AI tools that are adequately implemented can make significant improvements and simplifications in healthcare when it comes to safety, compliance, protecting patient trust, timely response, and efficiency.

Archana et al. [4] explores the integration of blockchain and artificial intelligence in healthcare and argues that these technologies are ideally suited to address critical challenges such as securing electronic health records (EHRs), ensuring data privacy, and enabling secure data transfers. Key findings are that these technologies have improved the protection of data transmission and digital records, improved the security of EHRs, and the efficiency of data handling in sensitive situations such as pandemics, which translates into improved healthcare reliability. By combining these technologies, they argue, it is realistic to address challenges such as data security, privacy, and decentralized computing, forming a robust framework for advancing healthcare. The adoption of private blockchains demonstrates a commitment to data protection, which contributes to better accessibility and efficiency in work. This combination of technologies promises to advance disease identification and treatment, as well as the overall efficiency of the healthcare system, while addressing important challenges in this field. Further research into advanced AI capabilities combined with blockchain could improve outcomes and shape the future of global healthcare, while ensuring data security, privacy, and fostering innovation.

Hu et al [8] addresses security challenges and recent advances in AI systems. While AI has demonstrated significant benefits in areas such as image recognition, healthcare, education, autonomous vehicles, finance, and medical diagnostics, AI-based systems are susceptible to various security threats throughout their lifecycle. These threats include sensor manipulation and scaling attacks during data collection and processing, as well as data poisoning and adversarial attacks during model training and deployment. The authors provide an overview of these security issues, tracing the lifecycle of AI systems, identifying threats at each stage, and summarizing appropriate countermeasures. They also discuss future challenges and opportunities in addressing AI security. The paper aims to provide a comprehensive roadmap for improving AI security.

Martinez et al. [9] highlights how modern technological advances, such as the Internet of Things (IoT), Big Data, and blockchain, are transforming the healthcare environment, introducing new improvements as well as complexities. The paper identifies key actors and architectural components of healthcare systems, as well as major security issues, including threats and attacks affecting the sector. The authors use the widely recognized MITRE ATT&CK framework to map these threats, which represents a significant contribution to the field. In addition, the paper outlines various security mechanisms for protecting healthcare systems, highlights major research directions in the literature, and provides a list of public datasets used for machine learning to improve healthcare security. Finally, it presents research challenges that need to be addressed in future studies. The conclusion is that this comprehensive review aims to provide a comprehensive insight into cybersecurity in healthcare, addressing existing solutions and emerging challenges.

Kshetri et al. [10] explores the application of blockchain technology in artificial intelligence (AI)-based healthcare systems to improve safety and security. It presents blockchain as a secure recordkeeping technology that can be applied in various fields, including healthcare. Due to its decentralization as its main advantage, this protection method ensures high security standards for critical medical data, while encouraging transparency. The study highlights how AI-enabled blockchain addresses existing challenges in healthcare systems, such as security vulnerabilities, operational inefficiencies, and security issues. In addition, it discusses the role of AI in healthcare and identifies potential areas for blockchain integration. The authors propose a model called healthAIChain, which uses a combination of AI and blockchain to improve patient data management and security in healthcare settings.

Ali [11] examines the growing role of artificial intelligence (AI) in the cybersecurity of healthcare systems and highlights how AI is changing the way organizations protect patient data from emerging threats. AI enables proactive risk prediction, thereby reducing the possibility of cyber-attacks, and helps identify weak points in systems. It also advances cryptographic techniques for data protection and ensures compliance with key security standards. Author says that blockchain technology is being used to improve data integrity, especially in the context of IoT and IoMT devices, while AI is strengthening methods for verifying user identities. While these innovations offer promising solutions to future threats, there are also challenges. It is necessary to further develop AI technologies to improve data protection and speed up the response to threats. Federated learning stands out as a significant advance that allows preserving patient privacy while improving data security. This article provides insight into the main benefits and challenges of integrating AI to improve cybersecurity in healthcare. The author also mentions that healthcare organizations must address ethical, legal, and technological challenges to maintain patient trust. The bottom line is that a balanced approach is necessary to harness the potential of AI while ensuring security and compliance in an increasingly dynamic digital health environment.

Ratnawita [12] explores the impact of artificial intelligence (AI) on cybersecurity, looking at its defensive capabilities and potential threats, such as deepfake attacks and AI-based cyberattacks. Deepfake technology, using Generative Adversarial Networks (GANs), enables realistic manipulation of video and audio content, which creates risks such as disinformation and fraud. The study, through a literature review and data analysis, indicates that traditional security measures are becoming ineffective against advanced AI attacks. As a solution, the integration of AI into cyber defence is proposed, including machine learning, Zero Trust Architecture (ZTA) and automated response systems. It highlights the need for an adaptive strategy that combines technology, regulation and education to reduce the risks of AI threats.

Mutalib et al. [13] provides a literature review on the protection of artificial intelligence (AI)-based healthcare systems using blockchain technology. Key findings include that there are techniques to defend against AI attacks, but they are specific to certain types of attacks, while even training AI is vulnerable to other attacks. Blockchain solves security and privacy issues in healthcare, enables medical data verification and user tracking, protects distributed learning on heterogeneous medical data, and eliminates issues like single points of failure and non-transparency in healthcare systems. Although research in this area is still in its early stages, the authors propose a framework that uses blockchain for AI applications in healthcare, including NLP, computer vision, and acoustic AI. The goal is to provide a global solution to all types of AI attacks in healthcare, but further research is needed to overcome existing limitations and challenges.

3. Discussion

The discussion surrounding modern healthcare security in the 4.0 era underscores the criticality of advancing beyond traditional, perimeter-based security models. With the convergence of interconnected devices, cloud computing, and decentralized systems, the conventional approaches are insufficient to address the adaptive nature of current cyber threats. In this context, the role of innovative security methods becomes even more important.

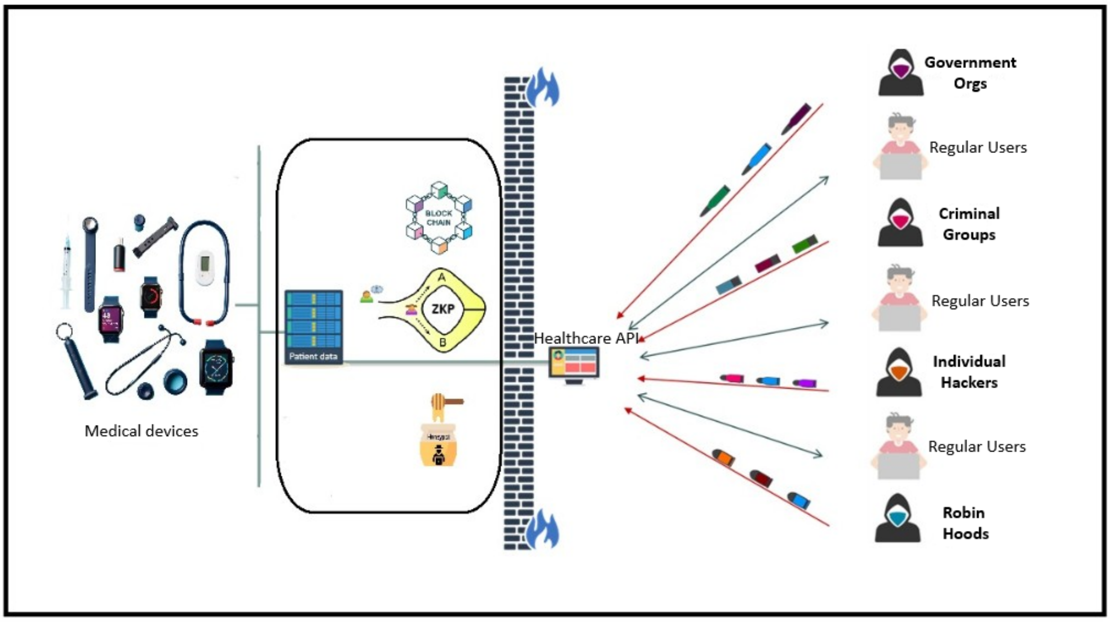

Figure 2. Our solution for data security in AI based healthcare applications.

The idea of this solution as we can see in Figure 2. is that even if there is a breakthrough or interception of communications between the patient and the application, our system, which can be a combination of blockchain, ZKP and honeypot, will be a security system for protecting the privacy of data of patients who use healthcare applications. Blockchain technology has a lot of promises when it comes to changing how healthcare data is managed. Because it's decentralized, it reduces the risk of a single point of failure and helps keep data secure and trustworthy. That said, putting blockchain into practice often runs into problems like limited scalability and high energy consumption [16]. To overcome these challenges, future work might focus on creating more energy-efficient ways for blockchains to reach consensus and combining blockchain with other technologies that complement it. Zero-knowledge proof offers a clever way to tackle a big challenge in healthcare: keeping patient information private while still proving that the data is accurate and trustworthy. This kind of cryptographic method is especially useful in fields where privacy rules are strict, and data is highly sensitive [17]. However, there's still work to be done to make zero-knowledge proofs faster and easier to integrate with existing healthcare databases without causing delays. Honeypot systems act as a kind of trap by pretending to be weak spots in a network. This helps IT teams study how attackers operate and prepare better defenses. But using honeypots in healthcare networks requires a careful balance-they need to be realistic enough to attract attackers but also controlled so they don't expose the system to unnecessary risks [18]. While honeypots can catch and log many attacks, they also generate a lot of alerts. This means teams need smart tools to sort through the noise and figure out which alerts are real threats, and which are harmless anomalies. When discussing these hybrid defense models, mixing different methods helps overcome the weaknesses each one has on its own. For example, combining AI powered honeypots with blockchain-based logging adds extra layers of security. This not only helps stop attacks but also makes it easier to investigate what happens if something goes wrong. Having this kind of backup is important for healthcare providers, as it helps them keep their services running smoothly-even when facing clever and persistent cyber threats.

3.1. Formatting of Mathematical Components of Our Hybrid Security System

To quantify the security of an AI-based healthcare system, we define a weighted hybrid model from a theoretical perspective:

- S: Overall security level of the AI-based healthcare system.
- B: Blockchain security contribution (data integrity and immutability).
- Z: Zero-Knowledge Proof (ZKP) contribution (data confidentiality and privacy).
- H: Honeypot contribution (detection and analysis of threats).
- α, β, γ: Weight coefficients representing the importance of each method, such that:

$$\alpha + \beta + \gamma = 1 \tag{1}$$

3.2. Hybrid Security Score

$$S = \alpha B + \beta Z + \gamma H \tag{2}$$

where each component is defined as a linear combination of contributing factors:

$$B = f_1(T, I) = \lambda_1 T + \lambda_2 I \tag{3}$$

$$Z = f_2(P, V) = \mu_1 P + \mu_2 V \tag{4}$$

$$H = f_3(D, A) = \nu_1 D + \nu_2 A \tag{5}$$

- T: Data traceability
- I: Immutability
- P: Privacy protection
- V: Verification accuracy
- D: Threat detection rate
- A: Adversarial behavior analysis
- $\lambda_i, \mu_i, \nu_i \in [0, 1]$: Scaling factors where $\sum \lambda_i = \sum \mu_i = \sum \nu_i = 1$

3.3. Explanation

- **Blockchain (*B*)** ensures that once data is recorded, it cannot be altered (immutability), and that every interaction is logged (traceability).
- **Zero-Knowledge Proofs (*Z*)** allow verification of computation without exposing underlying data, thereby enhancing privacy.
- **Honeypots (*H*)** serve as decoys to attract attackers and study intrusion techniques, improving adaptive response.

3.4. Use Case Scenario

- $B = 0.85$, $Z = 0.75$, $H = 0.65$
- $\alpha = 0.4$, $\beta = 0.4$, $\gamma = 0.2$

Then:

$$S = 0.4 \cdot 0.85 + 0.4 \cdot 0.75 + 0.2 \cdot 0.65 = 0.34 + 0.30 + 0.13 = \mathbf{0.77} \tag{6}$$

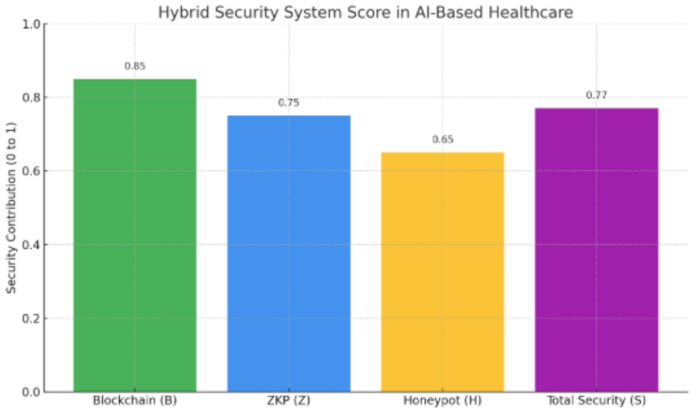

Figure 3. The overall security score of your hybrid system—combining Blockchain, Zero-Knowledge Proofs (ZKP), and Honeypots.

3.5. Future Work

The combination of AI and cybersecurity in healthcare opens up many promising research paths that could shape the future of digital medicine. As hospitals and clinics increasingly rely on interconnected systems and machine learning, there is a growing need to build smarter, more privacy ways to train AI models. One area of focus is federated learning, which allows different institutions to collaborate without sharing raw patient data. However, ensuring both privacy and model accuracy is tricky in today's world. Researchers are now exploring how tools like zero-knowledge proofs (ZKPs) and adaptive privacy controls can help solve this, along with better ways to protect against tampered data or compromised devices during model training. At the same time, it's crucial to prepare for future threats, especially those that could come from quantum computing and zero-day attacks. Many of the encryption techniques we rely on today, especially in blockchain systems, could be at risk in the coming years. Developing new forms of encryption that are safe against quantum attacks, and updating current systems to support them, will be an important step in securing long-term healthcare data. Another key area for future research is making AI in healthcare more transparent and trustworthy. Doctors and patients need to understand how AI tools make their decisions especially in high-stakes settings like diagnosis or treatment planning. This means creating models that are not just accurate but also explainable, even when they're operating in secure environments. Systems that can detect unusual behavior or signs of tampering, and then explain what's happening in clear terms, will go a long way in building trust. Honeypots, systems that act as decoys to attract cyber attackers can also become more effective if they evolve with the help of AI. In the future, we could see honeypots that automatically adapt based on how threats behave, making it harder for attackers to tell what's real and what isn't. These smart honeypots could help healthcare IT teams spot attacks early and learn from them faster. Beyond the technology itself, there's a growing need to create shared standards across countries and systems. As AI, blockchain, and cybersecurity solutions become more common in hospitals, everyone needs to agree on how data is handled, what security really means, and how to check if systems are meeting legal requirements. Smart contracts and blockchain logs could help automate some of this, but more research is needed to make these tools easier to use and more widely accepted. Advanced threats like deep fakes, data poisoning, and model manipulation will continue to evolve. Defending against them will take a mix of better AI models, cleaner training data, and tools that let people verify predictions without seeing the full dataset. Combining blockchain and ZKPs could help build systems where patients and doctors know they can trust what the AI is doing—without needing to see or share private data. Finally, as these tools are developed, we can't forget the human side. Security systems need to work for real doctors, nurses and patients who may not be tech experts. Making security tools easy to use and understand, while also respecting cultural and ethical differences, will be just as important as getting the technology right. And as healthcare increasingly goes mobile and global, researchers will need to think about how to make secure AI work on low-power devices, in rural areas, or during emergencies. In summary, while this paper lays the groundwork for a hybrid approach to securing AI-powered healthcare systems, there's a long road ahead. The future research work and implementation of security techniques will belong to those who can connect technical innovation with human-centered design, regulatory awareness, and a deep commitment to protecting patient trust in an increasingly digital world.

4. Conclusions

This review has examined the challenges and innovative security methods in the context of modern healthcare applications in the 4.0 era. The rapid growth of digital technologies has shown significant benefits in patient care and operational efficiency but has also expanded the vulnerability landscape and cybersecurity threats, exposing sensitive patient healthcare data to a multitude of adversarial threats. Our literature review and analysis reveal that while individual security measures such as blockchain, honeypots, and zero-knowledge proofs demonstrate considerable promise, their full potential is realized when deployed within a hybrid, adaptive security framework, including medical worker, policy maker and all responsible person in chain of healthcare systems. Future research should focus on developing more robust and explainable AI security techniques, exploring novel blockchain-zkp-honeypot based solutions, and establishing clear regulatory guidelines for data security in healthcare. Addressing the cybersecurity challenges in AI-based healthcare is not merely a technical issue but a fundamental requirement for ensuring patient safety, maintaining public trust, and realizing the full potential of AI to transform healthcare and data security.

Funding: This research was supported by the Science Fund of the Republic of Serbia, Grant No. 7502, Intelligent Multi-Agent Control and Optimization applied to Green Buildings and Environmental Monitoring Drone Swarms - ECOSwarm.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shinde, R.; Patil, S.; Kotecha, K.; Potdar, V.; Selvachandran, G.; Abraham, A. Securing AI-based Healthcare Systems using Blockchain Technology: A State-of-the-Art Systematic Literature Review and Future Research Directions. *arXiv preprint arXiv:2206.04793* **2022**.
2. Petrosino, L.; Masi, L.; D'Antoni, F.; Merone, M.; Vollero, L. A zero-knowledge proof federated learning on DLT for healthcare data. *Journal of Parallel and Distributed Computing* **2024**, *196*, 104992. https://doi.org/10.1016/j.jpdc.2024.104992.
3. Younis, F.; Miri, A. Using Honeypots in a Decentralized Framework to Defend Against Adversarial Machine-Learning Attacks. In *Lecture Notes in Computer Science*; 2019; pp. 24–48. https://doi.org/10.1007/978-3-030-29729-9_2.
4. Bathula, A.; Gupta, S.K.; Merugu, S.; Saba, L.; Khanna, N.N.; Laird, J.R.; Sanagala, S.S.; Singh, R.; Garg, D.; Fouda, M.M.; et al. Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. *Artificial Intelligence Review* **2024**, *57*. https://doi.org/10.1007/s10462-024-10873-5.
5. Arefin, S. Strengthening Healthcare Data Security with AI-Powered Threat Detection. *International Journal of Scientific Research and Management (IJSRM)* **2024**, *12*, 1477–1483. https://doi.org/10.18535/ijsrm/v12i10.ec02.
6. Gerardo, E. Healthcare Cybersecurity: Data Poisoning in the Age of AI, 2024. https://doi.org/10.47852/bonviewjcbar42024067.
7. Arefin, S.; Simcox, M. AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity. *International Business Research* **2024**, *17*, 74. https://doi.org/10.5539/ibr.v17n6p74.
8. Hu, Y.; Kuang, W.; Qin, Z.; Li, K.; Zhang, J.; Gao, Y.; Li, W.; Li, K. Artificial Intelligence Security: Threats and Countermeasures. *ACM Computing Surveys* **2021**, *55*, 1–36. https://doi.org/10.1145/3487890.
9. Martínez, A.L.; Pérez, M.G.; Ruiz-Martínez, A. A comprehensive review of the state of the art on security and privacy issues in Healthcare. *ACM Computing Surveys* **2022**. https://doi.org/10.1145/3571156.

10. Kshetri, N.; Hutson, J.; G, R. healthAIChain: Improving security and safety using Blockchain Technology applications in AI-based healthcare systems, 2023. arXiv preprint, https://doi.org/10.48550/arXiv.2311.00842.
11. Ali, M. Artificial Intelligence in Healthcare: Safeguarding Data and Enhancing Information Access through Cybersecurity. *Global Insights in Artificial Intelligence and Computing* **2025**, *1*, 57–80. https://doi.org/10.70445/giaic.1.2.2025.57-80.
12. Ratnawita, R. Cybersecurity in the AI Era Measures Deepfake Threats and Artificial Intelligence-Based Attacks. *Journal of the American Institute* **2025**, *2*, 180–189. https://doi.org/10.71364/s3emxx77.
13. Mutalib, N.H.A.; Sabri, A.Q.M.; Wahab, A.W.A.; Abdullah, E.R.M.F.; AlDahoul, N. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review. *Artificial Intelligence Review* **2024**, *57*. https://doi.org/10.1007/s10462-024-10890-4.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.