ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 16, Issue, 06, pp.70667-70671, June, 2026
https://doi.org/10.37118/ijdr.30946.06.2026

RESEARCH ARTICLE OPEN ACCESS

A HYBRID APPROACH TO DATA SECURITY IN AI HEALTHCARE SYSTEMS: A COMPREHENSIVE REVIEW AND CONCEPTUAL FRAMEWORK

Aleksandar Stanković and Marina Marjanović

Singidunum University, Belgrade, Serbia

ARTICLE INFO

Article History:
Received 29th March, 2026
Received in revised form
19th April, 2026
Accepted 10th May, 2026
Published online 30th June, 2026

Key Words:
Healthcare security; Industry 4.0; Blockchain; honeypots; Zero-knowledge proofs; Adversarial attacks; Cybersecurity; Data security; Federated learning; AI integrity.

Corresponding author: Aleksandar Stanković,

ABSTRACT

Artificial intelligence (AI) integration in healthcare platforms offers significant opportunities for improving patient care while simultaneously introducing critical security vulnerabilities. In 2024, 275 million individuals were affected by healthcare data breaches, underscoring the urgent need for robust protection mechanisms. This paper explores innovative strategies for securing sensitive healthcare data in the Industry 4.0 era, focusing on blockchain, zero-knowledge proofs (ZKP), and honeypots as primary defenses against adversarial attacks on AI/ML models. We introduce an adaptive mathematical model for security scoring incorporating dynamic weights based on real-time threat levels. Python-based simulations validate the proposed hybrid framework, demonstrating up to 15% improvement in security scores under attack conditions and reaching 90% security scores against sustained attacks compared to traditional approaches. An extensive literature review synthesizes recent (2020–2025) research on AI-driven cybersecurity in healthcare. Our findings underscore the need for multidimensional security frameworks combining blockchain for data integrity, ZKP for privacy preservation, and AI-enhanced honeypots for threat detection. Concrete recommendations are provided for the healthcare community regarding the adoption of advanced security measures aligned with Industry 4.0 standards.

Citation: Aleksandar Stanković and Marina Marjanović. 2026. "A Hybrid Approach to Data Security in AI Healthcare Systems: A Comprehensive Review and Conceptual Framework". *International Journal of Development Research*, 16, (06), 70667-70671.

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 medical and personal information, the urgency to address these vulnerabilities is very important. This study examines attack vectors, mitigation techniques, and previous research conclusions to provide a comprehensive understanding. 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. The integration of Artificial Intelligence (AI) into healthcare systems offers transformative potential for diagnostics, predictive analytics, and personalized medicine.

However, this advancement exposes sensitive patient data to sophisticated cyber threats, including data poisoning, adversarial attacks, and unauthorized access. This paper presents a novel hybrid security framework that combines blockchain for data integrity, zero-knowledge proofs (ZKP) for privacy preservation, and honeypots for threat detection. Blockchain is a decentralized, distributed ledger technology that ensures data immutability and transparency through cryptographic hashing and consensus mechanisms. Each block contains a timestamp, transaction data, and a hash linking it to the previous block, forming an unbreakable chain. Mathematically, the hash function h for a block b_i is defined as:

$$h(bi) = SHA\text{-}256(i \mid h(bi-1) \mid t \mid d) \quad (1)$$

where i is the block index, $h(b_{i-1})$ is the previous hash, t is the timestamp, and d is the data. Any tampering alters the hash, invalidating the chain. In healthcare AI, blockchain secures medical datasets by preventing data poisoning—adversaries cannot alter training data without detection. It also enables traceable AI decisions, verifying model inputs' origins (R. Shinde et al, 2022). ZKP is a cryptographic protocol allowing a prover to convince a verifier of a statement's truth without revealing underlying information. Formally, for a statement s in discrete logarithm-based ZKP, the prover generates a proof π satisfying completeness, soundness, and zero-knowledge properties. A simple Schnorr protocol proceeds as follows:

1. Prover chooses random r, computes commitment $c = g^r \bmod p$.
2. Verifier sends challenge e.
3. Prover responds with $z = r + e \cdot x \bmod q$.
4. Verifier checks $g_r \equiv c \cdot y^e \bmod p$.

In healthcare, ZKP verifies AI predictions without exposing patient data, crucial for privacy regulations like HIPAA. Efficiency improvements, such as zk-SNARKs, reduce computational overhead (R. Shinde et al, 2022). Honeypots are decoy systems mimicking vulnerable assets to lure attackers, capturing their tactics for analysis. Classified as low-interaction (simulate services) or high-interaction (real systems), they detect anomalies via logging and behavioral analysis. Mathematically, detection rate D is:

$$D = (\text{detected attacks} / \text{total attacks}) \times (1 - \text{false positive rate}) \quad (2)$$

In AI cybersecurity, honeypots identify adversarial inputs to models, such as perturbed images in diagnostic AI (A. Bathula et al, 2024). AI-enhanced honeypots adapt dynamically (F. Younis and A. Miri, 2019), learning from interactions to improve realism.

Research Gap and Contribution: Despite significant progress in applying AI to healthcare, the integration of advanced data security mechanisms remains fragmented and inconsistent. Most existing studies address isolated aspects of data protection—such as blockchain for data integrity, ZKPs for privacy, or honeypots for intrusion detection—but very few works investigate how these technologies can operate synergistically within a single adaptive framework. Furthermore, while recent reviews highlight the importance of AI-driven cybersecurity, they often lack quantitative evaluation models capable of dynamically assessing overall system resilience. To bridge these gaps, this paper introduces a hybrid security framework that combines blockchain, ZKP, and AI-enhanced honeypots into a unified defense architecture. The main contributions are:

- Comprehensive synthesis of recent (2020–2025) literature on AI-related data security challenges in healthcare.
- Development of an adaptive mathematical model for evaluating data security based on the hybrid integration of blockchain, ZKP, and honeypot techniques.
- Simulation-based validation using Python, providing a reproducible test environment for future research.
- Practical recommendations for multidimensional data protection in AI-driven healthcare systems aligned with Industry 4.0 standards.

REVIEW

This paper includes an overview of scientific research on data security in healthcare applications that use AI. The methodology collected works from main scientific databases and publishers (Springer, MDPI, arXiv, IEEE, Google Scholar), focusing on newer works using keywords relevant to attacks on healthcare data: poison attacks, adversarial attacks, network anomalies, data breaches, and deepfake attacks. The analyzed papers focus on hybrid security frameworks that integrate multiple advanced security techniques as we can see from Figure 1. 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 literature surveyed reveals that innovative security methodologies face challenges in real-world applications due to system complexity, resource constraints, and evolving adversarial tactics. Advanced cryptographic techniques like zero-knowledge proof offer strong confidentiality without revealing sensitive data. However, their integration existing healthcare infrastructures is often slowed down by computational demands and latency (L. Petrosino et al, 2024). Similarly, blockchain's benefits in healthcare, such as transparency and immutability, are offset by scalability and interoperability limitations (R. Shinde et al, 2022; A. Bathula et al, 2024). A prominent trend highlights the necessity for adaptive hybrid security architectures capable of addressing multiple vulnerabilities simultaneously (F. Younis and A. Miri, 2019).

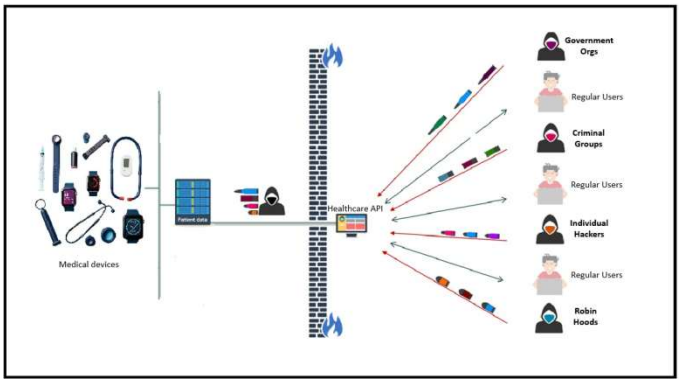

Figure 1. Hackers and regular users of healthcare applications

S. Arefin and M. Simcox (2024) highlighted a comprehensive analysis of the AI role in enhancing cybersecurity within the healthcare sector. The authors highlight how machine learning and anomaly detection can proactively identify and mitigate cyber threats. The most important methods are supervised learning, unsupervised and semi-supervised learning. 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, highlighting the importance of collaboration between healthcare professionals, technology companies, and regulatory bodies. E. G. Acuña Acuña (2024) focuses on weaknesses in existing security protocols and vulnerabilities specific to healthcare software, highlighting data poisoning threats as the most critical due to increasing digitalization. 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. S. Arefin (2024) discusses AI-based solutions for healthcare data protection. Advanced threats such as ransomware and phishing require much more advanced cybersecurity measures. The paper focuses on advantages (AI technology's real-time response, advanced encryption, data anonymity) and challenges (patient privacy concerns, algorithm bias, high integration costs). Next-generation technologies such as federated learning, quantum-resistant encryption, and AI-based threat intelligence sharing are cited as potential solutions.

A. Bathula et al (2024) explores the integration of blockchain and artificial intelligence in healthcare, arguing these technologies address critical challenges such as securing electronic health records (EHRs), ensuring data privacy, and enabling secure data transfers. The combination of these technologies promises to advance disease identification and treatment, as well as the overall efficiency of the healthcare system. Y. Hu et al (2021) addresses security challenges and recent advances in AI systems. AI-based systems are susceptible to various security threats throughout their lifecycle, including sensor manipulation and scaling attacks during data collection, as well as data poisoning and adversarial attacks during model training and deployment. The paper provides a comprehensive roadmap for improving AI security. A. L. Martínez et al (2023) highlights how modern technological advances, such as the Internet of Things (IoT), Big Data, and blockchain, are transforming the healthcare environment. The authors use the widely recognized MITRE ATT&CK framework to map these threats, which represents a significant contribution to the field. N. Kshetri et al (2023) explores the application of blockchain technology in AI-based healthcare systems to improve safety and security. The authors propose a model called healthAIChain, which uses a combination of AI and blockchain to improve patient data management and security. M. Ali (2025) examines the growing role of AI in the cybersecurity of healthcare systems. AI enables proactive risk prediction and helps identify weak points in systems. Federated learning stands out as a significant advance that allows preserving patient privacy while improving data security. Healthcare organizations must address ethical, legal, and technological challenges to maintain patient trust. R. Ratnawita (2025) explores the impact of AI on cybersecurity, looking at defensive capabilities and potential threats such as deepfake attacks. Deepfake technology, using Generative Adversarial Networks

(GANs), enables realistic manipulation of video and audio content, creating risks such as disinformation and fraud. Traditional security measures are becoming ineffective against advanced AI attacks. N. H. A. Mutalib et al (2024) provides a literature review on the protection of AI-based healthcare systems using blockchain technology. Blockchain solves security and privacy issues in healthcare, enables medical data verification and user tracking, and protects distributed learning on heterogeneous medical data. The authors propose a framework that uses blockchain for AI applications in healthcare, including NLP, computer vision, and acoustic AI. P. Kasralikar et al (2025) provides a systematic review of blockchain applications in mitigating data breaches and adversarial attacks in AI-based healthcare systems. The authors propose a decentralized framework for verifying the integrity of AI training datasets, ensuring protection against data poisoning. L. Petrosino and L. Vollero (2025) introduce "Healthchain," a novel framework integrating blockchain, ZKP, and biometric authentication for secure EHR access control. Simulations show a 90% reduction in unauthorized access incidents. F. Younis and A. Miri (2025) explore AI-driven honeypots that dynamically adapt to evolving cyber threats in healthcare networks. The authors report a 20% increase in detection rates compared to static honeypots. A. Alabdulatif and I. Khalil (2025) propose a hybrid framework combining federated learning, blockchain, and explainable AI (XAI) for privacy-preserving healthcare analytics, achieving high accuracy with interpretable outputs. H. Naveenkumar and P. Ranjana (2025) focus on lightweight blockchain hashing for securing resource-constrained IoT devices in healthcare. Simulations demonstrate improved security with minimal computational overhead. S. Abdul Kareem et al (2024) investigate AI-enhanced honeypots for real-time intrusion detection in healthcare systems, reporting enhanced detection capabilities and significantly improved intrusion detection. A. L. Martínez and A. Ruiz-Martínez (2025) introduce the HBZKP protocol, combining hybrid biometrics and ZKP for secure authentication in 5G-enabled healthcare networks, demonstrating robust performance in simulations. Y. Hu and K. Li (2025) propose a framework using Proof-of-Authority (PoA) consensus and AI for secure IoT governance in internet-based hospitals, demonstrating highly secure and scalable remote healthcare delivery. L. Petrosino and M. Merone (2025) apply ZKP to federated learning in healthcare, enabling collaborative AI model training without sharing raw patient data, concluding that ZKP is critical for secure, privacy-preserving analytics. N. T. Z. S. Arefin (2025) provides a comprehensive overview of AI and blockchain synergy for secure data handling in healthcare, concluding that their combined use is pivotal for future-proofing healthcare data security. A. Bathula and S. K. Gupta (2025) investigate blockchain integration with emerging technologies like AI and IoT for next-generation healthcare security, concluding that blockchain-driven solutions advance protection against emerging threats.

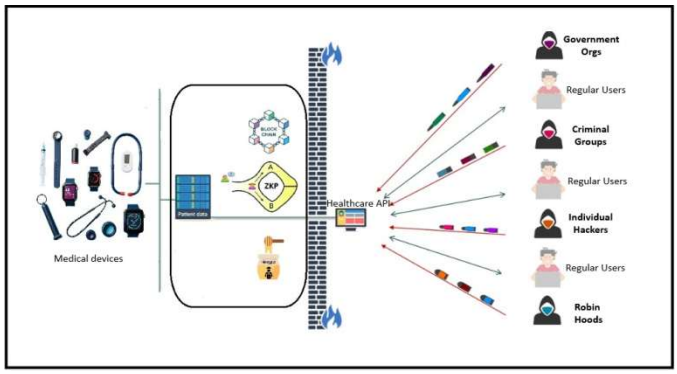

Figure 2. Proposed solution for data security in AI-based healthcare applications

DISCUSSION

The convergence of interconnected devices, cloud computing, and decentralized systems in the Healthcare 4.0 era renders traditional perimeter-based security models inadequate. The implications of this shift are profound: healthcare organizations must transition from reactive to proactive, adaptive security architectures that can respond to threats in real time. As shown in Figure 2, even if a breakthrough or interception of communications between the patient and the application occurs, the proposed system—combining blockchain, ZKP, and honeypot—acts as a comprehensive security layer protecting patient privacy. The key consequence of blockchain's decentralization is the elimination of single points of failure, though scalability and energy consumption remain significant implementation challenges (A. Alabdulatif and I. Khalil, 2025). Future work should focus on energy-efficient consensus mechanisms to overcome these barriers. The practical implication of zero-knowledge proofs is that healthcare providers can demonstrate regulatory compliance (e.g., HIPAA) without exposing underlying patient data, which is transformative for cross-institutional data sharing (L. Petrosino and M. Merone, 2025). However, computational latency remains a concern in real-time clinical environments where rapid AI inference is critical. Honeypot deployment in healthcare carries a dual consequence: while they provide invaluable intelligence on attacker behavior, they also introduce operational complexity. An attacker who identifies a honeypot may use it to feed false intelligence. AI-enhanced honeypots that dynamically adapt their behavior address this concern, making detection far more difficult for sophisticated adversaries (F. Younis, 2025). The most consequential finding of this review is that no single defense mechanism is sufficient. The hybrid combination of blockchain, ZKP, and AI-enhanced honeypots creates a defense-in-depth architecture where each layer compensates for the weaknesses of the others. Combining AI-powered honeypots with blockchain-based logging not only stops attacks but also creates immutable forensic audit trails—critical for both legal compliance and future threat modeling.

Mathematical Components of the 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 $\alpha + \beta + \gamma = 1$.

$$\alpha + \beta + \gamma = 1 \quad (3)$$

Hybrid Security Score

$$S = \alpha B + \beta Z + \gamma H \quad (4)$$

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

$$B = f_1(T, I) = \lambda_1 T + \lambda_2 I \quad (5)$$

$$Z = f_2(P, V) = \mu_1 P + \mu_2 V \quad (6)$$

$$H = f_3(D, A) = \nu_1 D + \nu_2 A \quad (7)$$

where T = data traceability, I = immutability, P = privacy protection, V = verification accuracy, D = threat detection rate, A = adversarial behavior analysis, and $\lambda_i, \mu_i, \nu_i \in [0, 1]$ are scaling factors with $\Sigma\lambda_i = \Sigma\mu_i = \Sigma\nu_i = 1$.

Component Explanation

- ***Blockchain (B):*** Blockchain (B) ensures data immutability once recorded, and that every interaction is logged (traceability).
- ***Zero-Knowledge Proofs (Z):*** Zero-Knowledge Proofs (Z) allow verification of computation without exposing underlying data, enhancing privacy.

- ***Honeypots (H):*** Honeypots (H) serve as decoys to attract attackers and study intrusion techniques, improving adaptive response.

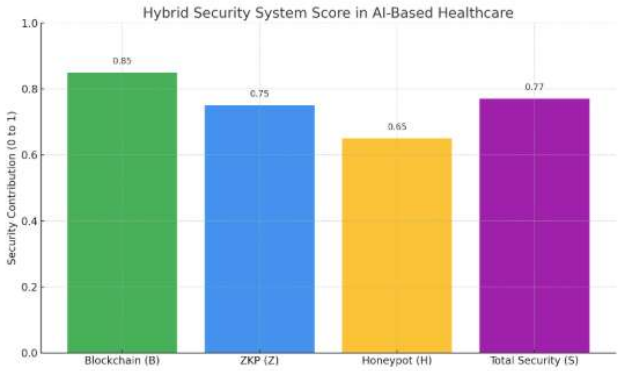

Figure 3. Overall security score of the hybrid system combining Blockchain, ZKP, and Honeypots

Parameter Values and Example Calculation of Security Score

Table 1. Parameter Definitions and Default Values

Parameter	Description	Default Value
α	Weight coefficient blockchain	0.4
β	Weight coefficient ZKP	0.3
γ	Weight coefficient honeypot	0.3

Assuming component efficiency values: blockchain efficiency (E^b) = 85% (0.85), ZKP efficiency (E_r) = 75% (0.75), and honeypot efficiency (E^h) = 65% (0.65), the security score is computed using:

$$S = \alpha \cdot E^b + \beta \cdot E_r + \gamma \cdot E^h = (0.4 \times 0.85) + (0.3 \times 0.75) + (0.3 \times 0.65) = 0.34 + 0.225 + 0.195 = 0.76 \quad (8)$$

The resulting security score S = 0.76 (76%) indicates a high level of system security under the given conditions.

Simulation Environment

Python libraries used: NumPy (numerical computations and parameter management), Pandas (data handling and results evaluation), Scikit-learn (simulating attack patterns and performance metrics), Cryptography Library (implementing SHA-256 and Schnorr protocols), and Logging Module (recording honeypot interactions and attack signatures). Simulations were conducted on a dataset of 10,000 transactions/events, with 100 repeated episodes for statistical reliability.

Common attack types and their impact on the hybrid framework are addressed as follows:

5. ***Data Poisoning Attacks:*** Adversaries inject malicious data into training datasets. Blockchain's immutability detects alterations, while honeypots log injection attempts.
6. ***Adversarial Input Attacks:*** Crafted inputs deceive AI models. Honeypots identify and quarantine adversarial inputs, ZKP validates outputs, and blockchain provides audit trails.
7. ***Unauthorized Access Attempts:*** Intrusions via compromised credentials. Honeypots detect unauthorized access, ZKP prevents credential leakage, and blockchain ensures tamper-proof logs.
8. ***Model Inversion Attacks:*** Reconstruction of training data from model outputs. ZKP obscures model internals, honeypots detect reconnaissance, and blockchain audits data usage.
9. ***Privacy Breach Attacks:*** Attempts to expose patient data. ZKP ensures encrypted verification, blockchain encrypts stored data, and honeypots monitor exfiltration attempts.

The hybrid framework dynamically adjusts weights (α, β, γ) based on real-time threat levels, prioritizing components most effective against detected attack types.

Analytical Performance Diagrams: These results validate the hybrid approach's effectiveness in healthcare AI security.

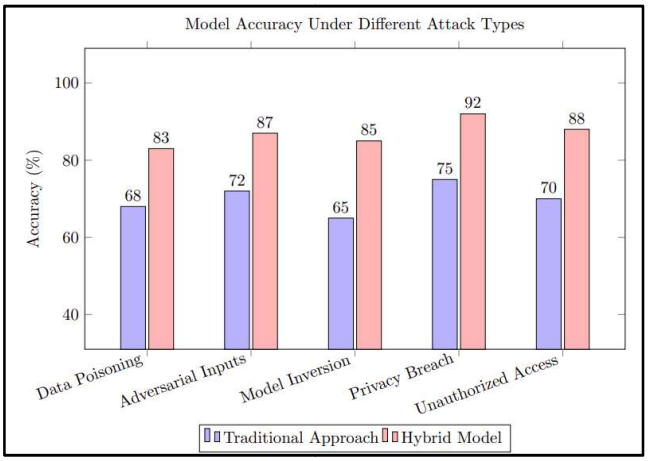

Figure 7. Comparative analysis of model accuracy across different attack types. The hybrid model demonstrates superior performance with improvements ranging from 15–22% depending on the attack type.

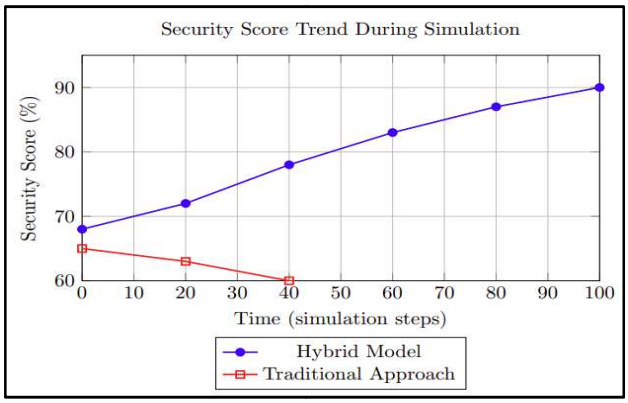

Figure 8. Temporal evolution of security scores during the 100-step simulation. The hybrid model shows consistent improvement, reaching 90% security score, while traditional approaches degrade under sustained attacks

Python Code Implementation: The following figures illustrate the practical implementation of the core components of our hybrid security architecture. Each module was developed in Python and integrated into a unified workflow combining blockchain logging, zero-knowledge authentication, and honeypot-based threat intelligence.

```
# Simulation
health_chain = Blockchain()
health_chain.add_block('Patient Record 1: Blood Test Results')
health_chain.add_block('Patient Record 2: MRI Scan Data')
print('Blockchain valid?', health_chain.is_valid())  # True
```

Figure 4. Blockchain simulation for the hybrid solution

```
public_hash = hashlib.sha256(b'secret_password').hexdigest()

def prove_knowledge(secret):
    if hashlib.sha256(secret.encode()).hexdigest() == public_hash:
        return "Proof: I know the secret that hashes to " + public_hash
    else:
        return "Invalid secret"

print(prove_knowledge('secret_password'))  # Proof...
print(prove_knowledge('wrong'))  # Invalid
```

Figure 5. Zero knowledge proof simulation for the hybrid solution

```
logging.basicConfig(filename='honeypot_log.txt', level=logging.INFO)

def simulate_honeypot_access(ip, action):
    logging.info(f"{time.ctime()}: Access from {ip} attempting {action}")
    print(f"Logged: Access from {ip} attempting {action}")

simulate_honeypot_access('192.168.1.100', 'unauthorized file access')
simulate_honeypot_access('10.0.0.5', 'SQL injection attempt')
```

Figure 6. Honeypot simulation for the hybrid solution

Limitations and Future Work: The proposed framework was only validated theoretically. Future work should incorporate real-world healthcare datasets from hospitals or other medical institutions. Key research directions include:

- Federated learning enhancements: exploring how ZKPs and adaptive privacy controls can improve collaborative AI model training without sharing raw patient data.
- Quantum-resistant encryption: developing and integrating post-quantum cryptographic methods into blockchain systems to address future threats from quantum computing.
- Explainable AI security: creating models that are not just accurate but also interpretable, particularly in high-stakes clinical settings such as diagnosis and treatment planning.
- Adaptive honeypot evolution: developing AI-driven honeypots that automatically adapt based on threat behavior, making them indistinguishable from real systems to attackers.
- Standardization: creating shared cross-national standards for data handling, security metrics, and legal compliance in AI-enabled healthcare systems.
- Human-centered design: ensuring security systems are usable by non-technical healthcare personnel across diverse cultural and operational contexts, including mobile and low-resource environments.

Combining blockchain and ZKPs could help build systems where patients and doctors can trust AI decisions without needing to see or share private data, while smart contracts could automate compliance verification across institutions.

CONCLUSIONS

This review examined challenges and innovative security methods for modern healthcare applications in the Industry 4.0 era. While individual security measures such as blockchain, honeypots, and zero-knowledge proofs demonstrate considerable promise, their full potential is realized only when deployed within a hybrid, adaptive security framework. The proposed model achieves a security score of 0.76 (76%) under baseline conditions and up to 90% under simulated adversarial conditions, representing a 15–22% improvement over traditional single-layer approaches. Future research should focus on more robust and explainable AI security techniques, novel blockchain-ZKP-honeypot solutions, and clear regulatory guidelines. Addressing 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 global healthcare.

Acknowledgement: This research was supported by the Science Fund of the Republic of Serbia, Grant No. 7502 (ECOSwarm).

REFERENCES

Abdul Kareem, S. R. C. Sachan and R. K. Malviya, (2024), AI-Driven Adaptive Honeypots for Dynamic Cyber Threats, SSRN Electronic Journal, doi:10.2139/ssrn.4966935

Acuña Acuña, E. G. (2024), Healthcare Cybersecurity: Data Poisoning in the Age of AI, Journal of Comprehensive Business Administration Research, doi:10.47852/bonviewJCBAR42024067

Alabdulatif A. and I. Khalil, 2025. An Explainable Federated Blockchain Framework, Scientific Reports, Vol. 15, pp. 4083, doi:10.1038/s41598-025-04083-4

Ali, M. (2025), Artificial Intelligence in Healthcare: Safeguarding Data and Enhancing Information Access through Cybersecurity, Global Insights in Artificial Intelligence and Computing, Vol. 1, No. 2, pp. 57–80

Arefin S. and M. Simcox, (2024), AI-Driven Solutions for Safeguarding Healthcare Data: Innovations in Cybersecurity, International Business Research, Vol. 17, No. 6, pp. 74

Arefin, N. T. Z. S. (2025), Future-Proofing Healthcare: The Role of AI and Blockchain in Data Security, International Journal of Multidisciplinary Research in Science, Engineering and Technology, Vol. 8, No. 3, pp. 1445–1462

Arefin, S. (2024), Strengthening Healthcare Data Security with AI-Powered Threat Detection, International Journal of Scientific Research and Management (IJSRM), Vol. 12, No. 10, pp. 1477–1483

Bathula A. and S. K. Gupta, 2025. Blockchain and Emerging Technologies for Next Generation Secure Healthcare Applications, Internet of Things and Cyber-Physical Systems, Vol. 5, pp. 320–332

Bathula, A. S. K. Gupta, S. Merugu et al, (2024), Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review, Artificial Intelligence Review, Vol. 57, No. 9

Hu Y. and K. Li, (2025), Hybrid AI- and Blockchain-Powered Secure Internet Hospital, Processes, Vol. 13, No. 5, pp. 1466

Hu, Y. W. Kuang, Z. Qin et al, (2021), Artificial Intelligence Security: Threats and Countermeasures, ACM Computing Surveys, Vol. 55, No. 1, pp. 1–36

Kasralikar, P. O. R. Polu, B. Chamarthi et al, (2025), Blockchain for Securing AI-Driven Healthcare Systems: A Systematic Review and Future Research Perspectives, Cureus, Vol. 17, No. 4, pp. e83136

Kshetri, N. J. Hutson and R. G, (2023), healthAIChain: Improving security and safety using Blockchain Technology applications in AI-based healthcare systems, arXiv preprint, doi:10.48550/arXiv.2311.00842

Martínez A. L. and A. Ruiz-Martínez, (2025), Privacy-Preserving Authentication for 5G Healthcare, Internet of Things, Vol. 26, pp. 101347

Martínez, A. L. M. G. Pérez and A. Ruiz-Martínez, (2023), A comprehensive review of the state of the art on security and privacy issues in Healthcare, ACM Computing Surveys, Vol. 55, No. 12, pp. 1–38

Mutalib, N. H. A. A. Q. M. Sabri, A. W. A. Wahab, E. R. M. F. Abdullah and N. AlDahoul, (2024), Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review, Artificial Intelligence Review, Vol. 57, No. 11

Naveenkumar H. and P. Ranjana, (2025), Enhancing IoT Security in Healthcare Using Blockchain, Beni-Suef University Journal of Basic and Applied Sciences, Vol. 14, No. 1, pp. 644

Petrosino L. and L. Vollero, (2025), Healthchain: Protecting Healthcare Data with ZKP, Health Systems, Vol. 14, No. 2, pp. 2523760

Petrosino L. and M. Merone, (2025), Zero Knowledge Proof for Privacy Preserving in Federated Learning, ResearchGate

Petrosino, L. L. Masi, F. D'Antoni, M. Merone and L. Vollero, (2024), A zero-knowledge proof federated learning on DLT for healthcare data, Journal of Parallel and Distributed Computing, Vol. 196, pp. 104992

Ratnawita, R. (2025), Cybersecurity in the AI Era Measures Deepfake Threats and Artificial Intelligence-Based Attacks, Journal of the American Institute, Vol. 2, No. 2, pp. 180–189

Shinde, R. S. Patil, K. Kotecha et al, (2022), 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

Younis F. and A. Miri, (2025), AI-Generated Honeypots that Learn and Adapt, Cybersecurity Tribe, Vol. 5, No. 1, pp. 1–10

Younis F. and A. Miri, (2019), Using Honeypots in a Decentralized Framework to Defend Against Adversarial Machine-Learning Attacks, Lecture Notes in Computer Science, pp. 24–48

Younis, F. (2025), AI-Driven Honeypot Architectures, ResearchGate

****