

Cross-Vertical Integration of AI, Blockchain, and IoT for Secure and Resilient Digital Health Ecosystems

George Suci
Research & Development Department
Beia Consult International
Bucharest, Romania
george@beia.ro

Cosmina Stalidi
Research & Development Department
Beia Consult International
Bucharest, Romania
cosmina.stalidi@beia.ro

Eduard-Cristian Popovici
Telecommunication Department
National University of Science and
Technology POLITEHNICA Bucharest
Bucharest, Romania
eduard.popovici@upb.ro

Abstract—The convergence of AI, Blockchain, and IoT technologies is reshaping cybersecurity paradigms across digital health ecosystems. This study investigates their integration as a unified framework to address cross-sector security challenges, improve risk detection, and enhance data protection. AI mechanisms enable real-time threat identification and adaptive response through machine learning, while Blockchain ensures integrity, traceability, and decentralized governance of medical data. IoT devices, critical for healthcare automation and remote monitoring, are secured through embedded anomaly detection and robust encryption schemes. A set of structured tables and diagrams outlines the roles, interactions, and technical dependencies of these technologies in layered cybersecurity architectures. In particular, we propose and analyze a reference model combining AI agents, secure IoT data channels, and Blockchain-based authorization protocols. The architecture supports autonomous response loops and cross-domain coordination. This work also identifies implementation challenges such as interoperability, resource constraints, and adversarial AI risks. The findings demonstrate how autonomous, explainable, and trust-enhancing security models can contribute to the sustainable and resilient digital transformation of the healthcare sector and other critical verticals.

Keywords—Cybersecurity, Adversarial AI, Blockchain, IoT Security, Digital Health Ecosystem

I. INTRODUCTION

The increasing digitization of healthcare systems has led to significant advancements in patient care, operational efficiency, and data-driven decision-making. However, this digital transformation has also introduced complex cybersecurity challenges, as healthcare organizations manage vast amounts of sensitive patient data and rely on interconnected medical devices. The proliferation of cyber threats, including ransomware attacks, data breaches, and unauthorized access, has underscored the need for robust security mechanisms to protect digital health ecosystems.

In response to these challenges, emerging technologies such as Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) have gained prominence as integral components of modern cybersecurity frameworks.

AI has demonstrated significant potential in cyber threat detection, risk assessment, and anomaly detection through

advanced machine learning algorithms and real-time predictive analytics. Blockchain technology offers a decentralized and immutable ledger system that enhances data integrity, secure access control, and transparency in healthcare information management. Meanwhile, IoT, which enables the seamless interconnectivity of medical devices, also introduces security vulnerabilities that require effective mitigation strategies to prevent unauthorized intrusions and data compromises.

The current paper presents the integration of AI, Blockchain, and IoT as a synergistic approach to strengthening cybersecurity in healthcare. Section II presents a comprehensive overview of recent advancements, with a particular focus on their applications in enhancing cybersecurity within healthcare infrastructures. Additionally, it examines ongoing research initiatives in the domain of AI adversarial methodologies, highlighting emerging approaches to mitigating adversarial attacks and strengthening the resilience of AI-driven security systems. Section III delves into AI-driven cyber threat detection and risk assessment, while Section IV examines Blockchain's role in secure data management and access control. Section V discusses IoT security challenges and strategies for mitigating vulnerabilities in interconnected medical devices. The article concludes with insights into future research directions and potential advancements in the intersection of AI, Blockchain, and IoT for cybersecurity in digital health ecosystems.

II. RECENT DEVELOPMENTS IN AI, BLOCKCHAIN, AND IoT FOR CYBERSECURITY IN HEALTHCARE

The convergence of Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT) has driven significant advancements in autonomous, decentralized, and adaptive security architectures. These technologies collectively enhance real-time threat detection, secure data management, and resilient healthcare infrastructures, moving beyond conventional perimeter-based defenses.

AI has become integral to proactive cyber threat detection, enabling real-time analysis of network traffic, anomaly detection, and automated incident response. Advanced machine learning models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNN-LSTMs), have demonstrated efficacy in detecting irregular patterns within Healthcare IoT (HIoT) ecosystems,

identifying unauthorized access, system failures, and potential breaches [1],[2]. Furthermore, self-learning and adversarially robust AI systems are being developed to enhance adaptive cybersecurity defenses and mitigate emerging AI-powered cyberattacks.

Blockchain technology plays a pivotal role in ensuring data integrity, decentralizing access control, and securing medical records [2]. By leveraging distributed ledger technologies (DLTs) and cryptographic hashing, blockchain creates an immutable framework for secure interoperability among healthcare stakeholders.

The integration of smart contracts enables automated authorization mechanisms, reducing human intervention and minimizing risks associated with insider threats. The development of hybrid blockchain models aims to enhance scalability and regulatory compliance, particularly in frameworks such as GDPR and HIPAA [3].

The increasing adoption of IoT-enabled medical devices has expanded cybersecurity vulnerabilities, necessitating advanced encryption protocols, AI-powered anomaly detection, and blockchain-based data validation. A significant innovation in IoT security is the emergence of Ambient IoT, which leverages ambient energy sources (radio waves, light, heat, and motion) for power.

This next-generation IoT framework improves scalability, cost-efficiency, and network resilience, while enhancing secure real-time communication through Bluetooth, 5G Advanced, and IEEE 802.11bp standards.

In order to better understand the transformative potential of emerging technologies in securing digital healthcare infrastructures, Table I provides a summarized overview of their primary roles, key innovations, and technical contributions.

TABLE I. INNOVATIONS AND ROLES OF EMERGING TECHNOLOGIES IN HEALTHCARE CYBERSECURITY

Technology	Purpose / Role	Key Innovations / Features
Artificial Intelligence (AI)	Real-time threat detection, anomaly detection, adaptive defense	CNNs, RNN-LSTMs, self-learning AI, adversarial robustness
Blockchain	Data integrity, decentralized access control, secure medical record management	Distributed Ledgers, Cryptographic Hashing, Smart Contracts, Hybrid Blockchain models
Internet of Things (IoT)	Medical device connectivity, real-time monitoring	Advanced encryption, AI anomaly detection, Blockchain validation, Ambient IoT (powered by radio waves, light, etc.)
Ambient IoT	Energy-efficient, resilient IoT communication	Bluetooth, 5G Advanced, IEEE 802.11bp standards
Integration of AI & Blockchain & IoT	Move towards intelligent, autonomous, zero-trust security architectures	Decentralized identity management, adaptive self-healing security, regulatory compliance (GDPR, HIPAA)

The integration of AI, Blockchain, and IoT is shifting healthcare cybersecurity towards autonomous, zero-trust, and self-healing architectures. AI-driven anomaly detection, coupled with blockchain-enhanced decentralized identity frameworks, strengthens secure access control and tamper-proof data sharing [4]. These advances mark a transition towards adaptive cybersecurity ecosystems, capable of mitigating evolving threats while ensuring compliance with regulatory mandates [2],[4].

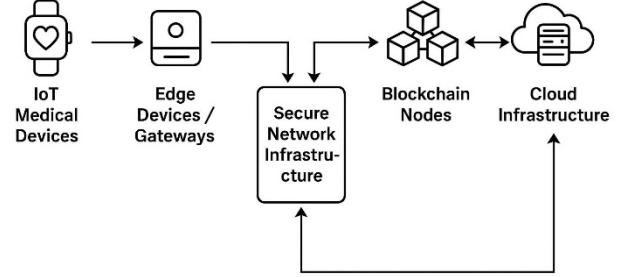


Fig. 1 Hardware architecture of the AI-Blockchain-IoT healthcare security system

The interplay between Artificial Intelligence (AI), Blockchain, and the Internet of Things (IoT), augmented by Ambient IoT technologies, lays the foundation for building autonomous, adaptive, and zero-trust cybersecurity ecosystems as illustrated in Figure 1. By leveraging these innovations, the next generation of cybersecurity in healthcare will move towards intelligent, autonomous, and highly resilient security frameworks, ensuring the integrity and privacy of digital health ecosystems.

III. ARTIFICIAL INTELLIGENCE-DRIVEN CYBER THREAT DETECTION AND RISK

The growing complexity and advancement of cyber threats have rendered traditional security measures inadequate for effectively safeguarding digital infrastructures. Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity, enabling enhanced threat detection, rapid response mechanisms, and adaptive risk mitigation strategies. AI-driven cybersecurity solutions leverage machine learning (ML), deep learning (DL), and advanced analytics to detect, predict, and neutralize evolving cyber threats in real time.

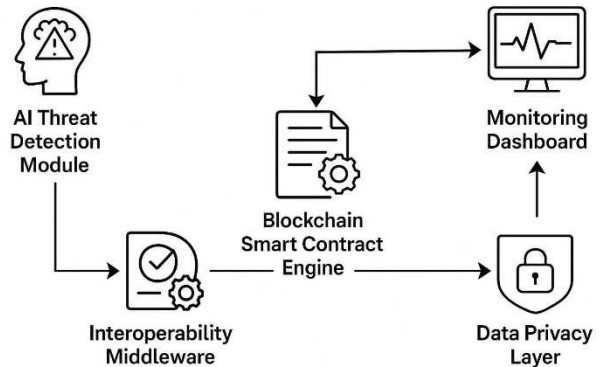


Fig. 2. Software modules and data flow in the integrated cybersecurity framework

However, while AI enhances defensive capabilities, it also introduces new risks and challenges, including adversarial attacks, data privacy concerns, and ethical dilemmas. Figure 2 provides an overview of the key software modules involved in this architecture, highlighting the data flow between AI-driven analytics, smart contracts and privacy-preserving layers.

A. AI cyber threat detection: Enhanced speed and accuracy

AI-driven cybersecurity systems provide an unparalleled advantage in detecting cyber threats with greater precision and efficiency than traditional rule-based approaches. AI models analyze vast datasets to identify patterns and anomalies that may indicate potential attacks, including malware infiltration, phishing campaigns, and zero-day vulnerabilities [5],[6]. Machine learning models are particularly effective in anomaly detection, allowing cybersecurity frameworks to identify deviations from normal network behavior without requiring

predefined signatures [5]. Supervised and unsupervised learning techniques are commonly employed to train AI models using historical attack patterns, enabling them to detect novel threats before they cause damage [5].

Furthermore, AI-powered automation enhances security operations by reducing response time. Automated AI-driven threat detection systems can instantly flag suspicious activity, isolate compromised systems, and trigger mitigation protocols without human intervention.[6] This shift from reactive to proactive security approaches significantly reduces attack surfaces and strengthens resilience against cyber threats.

B. The risks of AI in cybersecurity

Despite its advantages, AI-driven cybersecurity is not without risks (Figure 3).

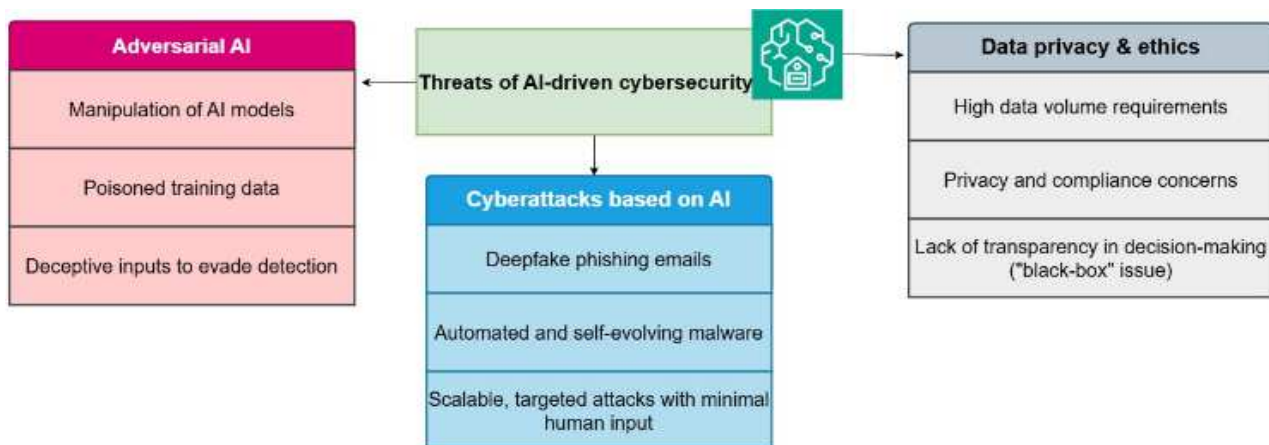


Fig. 3. Risks of AI-driven cybersecurity

One of the major concerns is adversarial AI, where attackers manipulate AI models through adversarial machine learning techniques, poisoning training data or crafting deceptive inputs to evade detection [7]. Cybercriminals can exploit AI's reliance on data patterns, leading to false negatives in detection systems, allowing complex malware and phishing attacks to bypass defenses.

Another risk factor is AI-powered cyberattacks, where threat actors leverage AI for offensive operations [7], [8]. AI-generated deepfake phishing emails, automated malware, and self-evolving attack scripts demonstrate how AI can be weaponized to compromise security infrastructures. The growing accessibility of AI tools enables cybercriminals to conduct large-scale, highly targeted attacks with minimal human intervention [8].

Data privacy and ethical concerns also pose significant challenges. AI-driven cybersecurity solutions require vast amounts of data for training and operation, raising concerns about user privacy and regulatory compliance [9]. The lack of transparency in AI decision-making processes, often referred to as the "black-box" problem, further complicates accountability and trust in AI-driven security measures.

C. Mitigating AI-Driven Cybersecurity Risks

To maximize the benefits of AI while minimizing risks, several strategies must be adopted:

- **Adversarial AI Defense Mechanisms:** Implementing robust machine learning models that can detect and mitigate adversarial attacks is crucial [10]. Techniques such as adversarial training, where models are trained with deceptive inputs, can help strengthen AI resilience.
- **Ethical AI Frameworks:** Establishing regulatory guidelines and ethical AI governance policies can ensure responsible AI deployment in cybersecurity [10].
- **Explainable AI (XAI):** Enhancing AI transparency through explainable AI models will improve trust and accountability in decision-making processes [10].
- **AI-Augmented Human Oversight :** While AI enhances threat detection, human analysts must remain an integral part of cybersecurity operations to validate AI-driven decisions and prevent errors [10].

IV. BLOCKCHAIN FOR SECURE DATA MANAGEMENT AND ACCESS CONTROL

The exponential growth of digital data across various domains, particularly in sensitive fields such as healthcare, finance, and smart governance, necessitates robust security frameworks. Conventional centralized data management systems are prone to security breaches, unauthorized access, and inefficiencies in access control. Blockchain technology has emerged as a transformative solution, offering decentralized, tamper-resistant, and transparent mechanisms for secure data management and access control [11]. Through cryptographic hashing, consensus mechanisms, and smart contracts, blockchain ensures data integrity, enhances privacy protection, and facilitates controlled access to sensitive information.

A. Decentralized access control mechanisms

Access control in traditional centralized systems relies on third-party intermediaries or regulatory bodies, making them vulnerable to security lapses and unauthorized data modifications. Blockchain, by design, eliminates such central points of failure by leveraging Decentralized Self-Sovereign Identity (SSI) and Role-Based Access Control (RBAC) models.

Self-Sovereign Identity (SSI): Blockchain enables users to have self-sovereign control over their identity and data. This model allows individuals to authenticate themselves securely without relying on centralized identity providers [11],[12]. Using decentralized identifiers (DIDs) and verifiable credentials, users can grant or revoke access to their data dynamically.

Access control enabled by smart contracts: Smart contracts facilitate automated, rule-based access control, ensuring that only authorized users can retrieve, modify, or share specific datasets [12]. These contracts execute predefined access policies autonomously, reducing human intervention and mitigating security risks.

Role-Based and Attribute-Based Access Control (RBAC & ABAC): Blockchain integrates RBAC and ABAC models, which assign permissions based on predefined roles (e.g., healthcare providers, researchers) or specific attributes (e.g., emergency access for critical conditions). This fine-grained access control enhances data privacy and ensures compliance with regulatory requirements [12],[14].

B. Ensuring Data Security and Integrity

Blockchain technology fortifies data security through its inherent immutability and cryptographic verification mechanisms. Every transaction recorded on the blockchain is hashed and linked to the previous block, making unauthorized modifications nearly impossible [13]. Key security benefits include:

- **Immutability:** Once a transaction is validated and added to the blockchain, it cannot be altered retroactively, ensuring an unforgeable audit trail.
- **Data Encryption and Anonymization:** Blockchain-based systems implement advanced encryption

techniques such as zero-knowledge proofs and homomorphic encryption to protect sensitive data while allowing authorized queries [15].

- **Decentralized Storage Solutions:** Many blockchain implementations utilize off-chain storage (e.g., InterPlanetary File System (IPFS)) to manage large datasets while storing only critical metadata on-chain, ensuring security without scalability trade-offs. [15]

V. IOT SECURITY AND VULNERABILITY MITIGATION IN HEALTHCARE

The integration of the Internet of Things (IoT) in healthcare has revolutionized patient monitoring, diagnostics, and medical data management. IoT-enabled medical devices, such as wearable sensors, smart implants, and real-time health monitoring systems, offer substantial benefits in terms of operational efficiency, personalized treatment, and accessibility [16],[17]. However, these advancements come with significant security challenges, including data privacy concerns, cyber threats, and system vulnerabilities that could compromise patient safety and healthcare infrastructure.

A. Security Challenges in Healthcare IoT Systems

IoT devices in healthcare are inherently vulnerable due to their interconnectivity, resource-constrained nature, and reliance on wireless communication networks [17]. The key security threats include:

- **Unauthorized access and data breaches:** IoT-based medical devices collect and transmit sensitive patient data, making them prime targets for cybercriminals. Unauthorized access to these systems could lead to identity theft, manipulation of medical records, and even malicious interference in medical treatments [17].
- **Network attacks and interception:** IoT devices rely on wireless communication protocols, including Wi-Fi, Bluetooth, and 5G networks, which are susceptible to attacks such as Man-in-the-Middle (MitM) attacks, denial-of-service (DoS), and ransomware threats. These attacks can disrupt real-time healthcare services, delay medical responses, or compromise device functionality [17].
- **Device hijacking and malware infections:** Many IoT medical devices operate on outdated or insecure software, susceptible to malware infections and botnet attacks. Attackers can hijack devices such as pacemakers, insulin pumps, and infusion pumps, posing life-threatening risks to patients [17].
- **Weak authentication and credential management:** Many healthcare IoT systems suffer from poor credential management practices, including hardcoded passwords, lack of multi-factor authentication (MFA), and insecure key management systems. [17] These vulnerabilities increase the likelihood of unauthorized access to critical medical infrastructure.
- **Interoperability and compliance issues:** Healthcare IoT systems must comply with stringent

regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) to ensure data security and privacy [17]. However, the lack of standardized security protocols across different IoT manufacturers is a challenge to regulatory compliance.

B. Mitigation strategies for healthcare IoT security

Companies in the healthcare sector must employ comprehensive security measures that include device-level, network-level, and system-wide defenses to mitigate these risks. Implementing advanced data encryption and secure communication protocols is crucial for protecting IoT networks in healthcare. Utilizing end-to-end encryption standards such as AES-256 and TLS 1.3 ensures the confidentiality of transmitted data, while blockchain-based secure data management systems further enhance data integrity and prevent unauthorized modifications. In addition, a zero-trust architecture for access control should be adopted, requiring continuous verification of all users, devices, and applications before granting access to sensitive healthcare data [18]. Role-based and attribute-based access control (RBAC/ABAC) mechanisms provide additional layers of security by restricting unauthorized access based on predefined rules and attributes. Table II summarizes the key categories, mitigation strategies, and security measures necessary to protect healthcare IoT devices and networks.

To strengthen anomaly detection and threat mitigation, AI and machine learning algorithms should be employed to analyze network traffic patterns and detect deviations that may indicate cyberattacks. AI-driven intrusion detection and prevention systems (IDPS) enable real-time monitoring and automated responses, improving overall cybersecurity resilience [17], [18]. Moreover, ensuring regular firmware and software updates is critical; healthcare organizations must enforce automated patch management systems to keep IoT devices updated with the latest security patches, while legacy systems should either be phased out or reinforced with additional security layers.

TABLE II. SECURITY FRAMEWORK FOR PROTECTING HEALTHCARE IoT DEVICES AND NETWORKS

Category	Mitigation strategy	Description
Security at the device level	Augmented data encryption	Implement end-to-end encryption standards such as AES-256 and TLS 1.3 to ensure the confidentiality of transmitted data.
	Secure identity and authentication mechanisms	Use multi-factor authentication (MFA), biometric verification, and blockchain-based decentralized identity (DID) solutions to prevent unauthorized access.
	Regular firmware and software updates	Enforce automated patch management systems to keep devices updated and secure, and strengthen legacy systems or phase them out.
Network security at the systemic level	Artificial intelligence-based anomaly detection and	Deploy AI and machine learning algorithms to monitor network traffic, detect cyber threats, and enable real-time automated responses through IDPS systems.

	threat mitigation	
	Network segmentation	Isolate IoT medical devices within dedicated network segments to prevent lateral movement of threats and minimize the attack surface.
Holistic protection mechanisms	Zero-Trust architecture	Adopt a zero-trust model requiring continuous verification of users, devices, and applications before granting access to sensitive healthcare data.
	RBAC and ABAC Mechanisms	Implement Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to restrict access based on predefined roles and attributes.
	Secure data management via blockchain technology	Utilize blockchain systems to enhance data integrity and prevent unauthorized modifications.
Regulatory compliance	Compliance with security standards and frameworks	Maintain compliance with ISO/IEC 27001, NIST Cybersecurity Framework, and IEC 80001 to ensure adherence to industry best practices in IoT security.

To further mitigate risks, secure identity and authentication mechanisms should be implemented, including multi-factor authentication (MFA), biometric verification, and blockchain-based decentralized identity (DID) solutions, all of which reduce the likelihood of unauthorized access to medical IoT devices. Establishing a resilient network infrastructure and segmentation also plays a key role in cybersecurity, as isolating IoT medical devices within dedicated network segments prevents lateral movement of threats and reduces the attack surface [18].

Finally, maintaining compliance with regulatory frameworks and security standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, and IEC 80001 is essential for ensuring that healthcare organizations adhere to best practices in IoT security [18]. By integrating these measures, healthcare institutions can fortify their cybersecurity posture and safeguard patient data from emerging threats.

C. Future Directions

Future research and development must prioritize addressing existing challenges by fostering interdisciplinary innovation and enhancing the security, efficiency, and ethical deployment of AI, Blockchain, and IoT technologies. One critical area requiring further exploration is AI transparency and explainability [19]. The adoption of Explainable AI (XAI) is essential to increasing trust and accountability in AI-driven decision-making systems. Future advancements should focus on the development of interpretable deep learning models capable of providing insights into the reasoning behind their outputs, particularly in high-stakes domains such as medical diagnostics and cybersecurity threat detection.

In parallel, adversarial AI defense and cybersecurity improvements must be pursued to counteract the growing sophistication of AI-powered cyber threats. The development of self-healing AI systems, which can detect and mitigate adversarial attacks in real time, would significantly enhance

cybersecurity resilience. Additionally, the integration of Zero Trust Architecture (ZTA) with AI-based threat detection could help defense mechanisms against evolving threats. [20]

Given the high computational demands of AI-driven applications, the development of scalable and energy-efficient AI models remains an important research focus. Future advancements should emphasize quantized deep learning techniques, federated learning, and low-power AI chips, which can reduce energy consumption while maintaining high accuracy in critical areas such as healthcare diagnostics and industrial automation. Similarly, blockchain technology for secure and interoperable data management presents another promising avenue for research [19], [20]. The implementation of hybrid blockchain models that balance scalability, decentralization and blockchain-based identity verification systems, could enhance data privacy and ensure regulatory compliance, particularly in healthcare and financial industries.

To address vulnerabilities in IoT security and healthcare applications, strengthening security measures is imperative to prevent unauthorized access and mitigate privacy concerns. Future work should explore the development of lightweight cryptographic protocols, blockchain-enhanced IoT security, and AI-powered anomaly detection systems that enable real-time threat monitoring in healthcare environments [21]. Additionally, Edge AI, which facilitates local AI processing on IoT devices, should be further developed to enhance real-time decision-making and reduce latency in critical applications such as remote patient monitoring.

Establishing comprehensive regulatory frameworks and ethical AI governance is essential to ensuring the responsible deployment of AI and cybersecurity solutions. Future research should investigate policy-driven AI governance models that balance innovation with privacy and regulatory compliance. The implementation of AI fairness audits and bias-mitigation techniques should also be prioritized to eliminate discriminatory outcomes in AI-driven decision-making systems [22]. Moreover, AI-enabled predictive analytics offers significant potential in crisis management, cybersecurity threat prediction, and food supply chain optimization.

As AI-driven automation continues to transform industries, human-AI collaboration and workforce development must be emphasized. Research should explore models in which AI augments human expertise rather than replacing it, ensuring that AI-powered decision support systems in healthcare, cybersecurity, and industrial applications enhance human productivity while maintaining ethical oversight [19], [23].

By integrating these advancements across multiple domains, the future of AI, Blockchain, and IoT technologies will be characterized by greater security, efficiency, and ethical responsibility, driving innovation while safeguarding societal interests.

VI. CONCLUSIONS

As AI, Blockchain, and IoT continue to drive digital transformation, their integration must be approached with a strategic balance between innovation, security, privacy, and

ethical considerations. Addressing scalability constraints, regulatory compliance, and adversarial risks will be essential in ensuring the development of transparent, secure, and resilient AI-driven cybersecurity frameworks across healthcare and other critical sectors.

Future advancements should focus on enhancing explainability in AI-driven security systems, optimizing blockchain interoperability, and strengthening IoT security through decentralized and energy-efficient architectures. The evolution towards autonomous, zero-trust, and self-defensive cybersecurity ecosystems will require interdisciplinary collaboration among researchers, policymakers, and industry stakeholders. Ensuring responsible deployment, ethical governance, and regulatory alignment will be key to maximizing the benefits of these technologies while safeguarding critical digital infrastructures and protecting sensitive data in an increasingly connected world.

ACKNOWLEDGMENT

This project has received funding from the European Union under HORIZON-TMA-MSCA-SE, Topic HORIZON-MSCA-2022-SE-01-01, Grant Agreement No 101131292 (AIAS). This work was also supported by a grant of the European Commission, CHIPS Joint Undertaking (G.A. no. 101111977) and of the Ministry of Research, Innovation, and Digitization, CNCS/CCCDI - UEFISCDI, project number PN-IV-P8-8.1-PME-2024-0033 „Arrowhead Rețele flexibile de valorizare a producției”, within PNCDI IV.

REFERENCES

- [1] Akinade, S. K. (2024). Implementing AI-Driven Anomaly Detection for Cyber-security in Healthcare Networks. *ATBU Journal of Science, Technology and Education*, 12(2), 598-610. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [2] Wassan, S., Dongyan, H., Suhail, B., Jhanjhi, N. Z., Xiao, G., Ahmed, S., & Murugesan, R. K. (2024). Deep convolutional neural network and IoT technology for healthcare. *Digital health*, 10, 20552076231220123.
- [3] Amin, M. A., Tummala, H., Mohan, S., & Ray, I. (2023). Healthcare Policy Compliance: A Blockchain Smart Contract-Based Approach. *arXiv preprint arXiv:2312.10214*.
- [4] Ali, S., Abdullah, Armand, T. P. T., Athar, A., Hussain, A., Ali, M., ... & Kim, H. C. (2023). Metaverse in healthcare integrated with explainable AI and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors*, 23(2), 565.
- [5] Cyber threat detection using AI. (2024). *International Journal of Multidisciplinary Research and Explorer*, 4(1), 28-37.
- [6] Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, 7(12), 25-43.
- [7] Chittibala, D. R. (2024). Threat model detection using AI. *International Journal of Artificial Intelligence Research and Development (IJAIIRD)*, 2(1), 40-47.
- [8] Shahidi, S., Darmel, F. A., Jalalzai, S., & Amiri, G. A. (2024). Opportunities and Challenges in AI-Driven Cybersecurity: A Systematic Literature. *Journal of Social Science Utilizing Technology*, 2(4), 516-530.
- [9] Pragyans Das, Ishika Gupta, Sushruta Mishra, Chapter 10 - Artificial intelligence driven cybersecurity in digital healthcare frameworks, Editor(s): Deepak Gupta, Aboul Ella Hassanien, Securing Next-Generation Connected Healthcare Systems, Academic Press, 2024, Pages 213-228, ISBN 9780443139512,

- [10] Hassan, Syed Minhaj Ul Hassan, Study of Artificial Intelligence in Cyber Security and the emerging threat of AI-driven cyber attacks and challenge (July 17, 2023).
- [11] K. Azbeg, O. Ouchetto and S. Jai Andaloussi, "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management," in *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1515-1527, Aug. 2023, doi: 10.1109/TCSS.2022.3186945.
- [12] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras and J. H. M. Emati, "DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data," in *IEEE Access*, vol. 10, pp. 101011-101028, 2022, doi: 10.1109/ACCESS.2022.3207803.
- [13] Sonkamble RG, Bongale AM, Phansalkar S, Sharma A, Rajput S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics*. 2023; 12(4):1015.
- [14] Rana SK, Rana SK, Nisar K, Ag Ibrahim AA, Rana AK, Goyal N, Chawla P. Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare. *Sustainability*. 2022; 14(15):9471.
- [15] E. R. D. Villarreal, J. García-Alonso, E. Moguel and J. A. H. Alegría, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," in *IEEE Access*, vol. 11, pp. 5629-5652, 2023,
- [16] M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," in *IEEE Access*, vol. 11, pp. 145869-145896, 2023, doi: 10.1109/ACCESS.2023.3346320.
- [17] Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M. et al. Security vulnerabilities in healthcare: an analysis of medical devices and software. *Med Biol Eng Comput* 62, 257–273 (2024).
- [18] Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. *Sensors*. 2023; 23(21):8944.
- [19] Almotairi, K.H. Application of internet of things in healthcare domain. *J. Umm Al-Qura Univ. Eng.Archit.* 14, 1–12 (2023).
- [20] Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, 4(4), 17-27.
- [21] Hossein Omidian, Synergizing blockchain and artificial intelligence to enhance healthcare, *Drug Discovery Today*, Volume 29, Issue 9, 2024, 104111.
- [22] Husnain A. Artificial Intelligence and Deep Learning in Healthcare, Cyber security, and Food Systems: A Comprehensive Review of Applications, Challenges, and Future Directions. *Glob. J. Emerg. AI Comput.* [Internet]. 2025 Feb. 28 [cited 2025 Mar. 8];1(2):95-126.
- [23] Shinde, Y. A. A Comprehensive Survey on Enhancing Blockchain Data Security through the Integration of IoT and AI. *Journal of technical education*, 167.