International Journal of Emerging Research in Applied Medical Sciences (IJERAMS)

AI-Driven IoT Security Enhancements Using Blockchain Technology: A Data-Driven Approach

Sai prasanna Pilli
Malineni Lakshmaiah college of Pharmacy,telangana,india
saiprasannakumar305@gmail.com

ABSTRACT

The utilities of the IoT devices that industries are currently using are increasing at a very alarming rate based on the latest statistics meaning that very large figures of security issues are raised in terms of management and safeguarding of information. The traditional security systems would fail in an IoT network whereby more and more objects would connect to each other to generate massive amount of data. The paper will discuss the ways in which embracing Artificial Intelligence (AI) and Blockchain can enhance security of the IoT. Artificial Intelligence can identify bug lapses, prevent infiltrations and provide predictive security claims and Blockchain can secure messages and guarantee data continuity and decentralized loyalty. The AI based and blockchain used security protection comes with the security protection provided by the proposed IoT security protection that gives the real time identification and efficacy of the IoT security threats in the IoT systems. In this context, the use of data-driven approach can be implemented and this aspect in itself makes this framework dynamic as pertains to the security environment. This way, it provides a decent cover to a variety of hazards. The paper now looks into realities on how this holistic approach can be applied in the real life of actual implementation of the same in the real life of actual implementation of the IoT system and how effective it can go to the point of making the IoT systems more efficient in the realms of enhancing the security and scalability of the IoT systems. Any case on information theft, unauthorized access to the systems and vulnerability of systems are traced the answer as the results of the experiment show that the AI and Blockchain will be able to provide powerful tool in the securing of IoT devices.

Keywords: ***AI, Blockchain, IoT, Security, and Anomaly detection, Data Integrity.***

DOI: https://doi.org/10.65477/ijerams.v1.i1.05

1. Introduction

The proposed framework, functionality and the components of the same have also been sufficiently presented in the paper with a focus as to how the proposed AI based threat detectors systems and the security measures to be underpinned by the Blockchain can consequently serve to complement one another in preventing as many IoT specific attacks and vulnerabilities as

possible. Such a measure can augment the integrity and confidentiality of data on the IoT network (Tauseef et al., 2023). The need in such interrelation emerges when one talks about the growing interest in the requirements of trustful and secure products within the context of the rapid modernization of the digital world (Kuznetsov et al., 2024).

The authors also strive to cover the gap in the range of research devoted to the matter because the existing researches are devoted to the safety of issues, which correlate with the union of AI-Blockchain and are interesting to a researcher as well as a practitioner (Kuznetsov et al., 2024). Specifically enough, the article discusses the benefits of AI and Blockchain united, and it as well speculates on the potential menaces to the security (not to mention the subsequent measures as far as implementation of the acquisitions is concerned) (Kuznetsov et al., 2024) (Tauseef et al., 2023). It will be able to address the privacy of the sensitive data, integrity of systems and trust in the use of IoT (Shanmugam et al., 2023) (Nasayreh et al., 2024). IT framework performance will also be followed in detail by simulations and real-life situations reflecting the way it may be used in detection and prevention of cyberattacks, data integrity, and the possibility of the easy running of the IoT system, in general (Chen et al., 2024) (Nasayreh et al., 2024).

2. Background of the study

The other notion in the article is the Internet of Medical Things as the sub-type of the IoT, which is focused on the medical equipment connected to the Internet and the transfer of confidential information of the patient (Nasayreh et al., 2024). One of the most vivid tendencies discovered with regard to the rapid introduction of the IoT in the healthcare sector referred to the fact that not only the establishment of the improved efficiency of the activities and favourable patient outcomes it was linked to the emergence of the significant security risks and confidentiality challenges in healthcare (Nasayreh et al., 2024). The privacy of the customers and the institutions and the competition do not stimulate the intention to make data by the medical institutions (Zhu & Li, 2025). It is also aggravated by the fact that there is also a rise in cyber-attacks against health resources and this could impact both the patients and the medical staff (Suleski et al., 2023) (Nasayreh et al., 2024). This type of attack is very threatening, the data which has already been published in the medicine sector is sensitive, and the prospective assailants can have an opportunity to interfere with the medical equipment (Nasayreh et al., 2024) (Dou et al., 2025).

The diversity of the environment of healthcare IoT in terms of various kinds of different devices, various kinds of communication protocols, various kinds of security needs and implementations, is gigantic and this is characteristic can introduce the possibility of potential and unmitigated vulnerability in which malicious users can exploit (ElSayed et al., 2025). Their solution can also be traced in the light of the potential of the safety and security of the information of patients (Al-Shargabi & Abuarqoub, 2020) (Clarke & Martin, 2023). Artificial intelligence and blockchain are the domains that were still unexplored that can be used to enhance security and privacy problems in the field of health care and offer it to the non-manipulating and decentralized environment where it can transfer its identities and protect its sources of information (Chen et al., 2024) (Meisami et al., 2023).

3. Justification

The second question which is reproduced in the research is the increase of the volume of a request construction of safe answers to consider IoT issues that can be presented in various markets including healthcare market, a financial market, and smart city market and to develop suggestions to propose a new situation that one can use to fight against the problem. To the best of our knowledge, the combination of AI and Blockchain will give rise to the rare opportunity to strengthen a given IoT environment against the ever-increasing threats (Tauseef et al., 2023). The space of interest is based on the prospects of using in real-time anomaly diagnosis, predictive analytics capability of AI and decentralized improvable ledger of Blockchain in securing an IoT network, and receiving the privacy of the user (Tauseef et al., 2023). Besides enacting such a synergy to support data integrity, such a synergy is also deployed to support the belief, the clarity, as well as the IoT devices and users (Martfnez et al., 2024) (Chen et al., 2024).

The fact is particularly relevant now, as the volume at which AI and the Blockchain technology is applied in different applications is continuously growing (Kuznetsov et al., 2024). With this sort of integration, the data security, transparency and experience might be promoted, which would result in a secured table, where the IoT products would be capable of coming forth and transfer a data (Hassan et al., 2024). The fact that Blockchain can verify integrity, transparentness as well as trustfulness of information implies that it is the most appropriate type (Bobde et al., 2024), which

is one of the significant requirements in the software that is going to be interacting with sensitive industrial data. The blending of AI and Blockchain brings the opportunities in the ways of cooperation to overcome the problems of the safety of the IoT systems, its ethics, and trust, which is the key to the possibility to receive the benefits and limit the risks of work with it safely (Kuznetsov et al., 2024) (Chen et al., 2024).

4. Study Purposes

To remark on the feasibility of rolling out AI in IOT systems to be able to grow in terms of AI-based security with its prospects to detect abnormal behaviour in real time, make a forecast according to the basis of threat, and be automated into one of the elements of response.

To deliberate on the future implication of implementing the Blockchain technology to realize the security of data transmitted, data integrity and decentralized trust in the networks of IoT.

To propose the framework, according to which IoT systems can be structured and made secure against the most popular security threats with the assistance of Blockchain.

It can be verified through its simulations and determining a case study of its implementation and usage in the given my proposed framework of IoT environment to measure its performance and also compare it with the real life scenario to measure its performance in preventing the cyber-attacks to maintain the data security.

To determine the problems that the realization of the AI and Blockchain with the IoT security poses and suggest the solutions that could be provided.

5. Literature Review

The proposal of blockchain technologies remains a new solution to the problem of the security and privacy of the IoT (Wang et al., 2021). The blockchain has a potential to offer information integrity, decentralized trust, and security of information within the systems of the IoT (Khordadpour & Ahmadi, 2024). It also has the capability to offer non-centralized and unforgeable system which will be in a position to ensure the confidentiality of the information in IoT (Tauseef et al., 2023). Another option that can be used to maintain safe industrial information with such features as calm information, transparent and faithful information (Bobde et al., 2024) is blockchain. The blockchain technology has demonstrated that it can be applied to control security attacks such as the Distributed Denial of Service attacks (Chen et al., 2024).

Among the benefits of the systems built on the blockchain technology, one can highlight the fact that the technology allows carrying out a credible transaction in the decentralized environment that continues to gather momentum in the data and transaction security landscape as Web 3.0 enters the picture (An et al., 2023) (Iqbal et al., 2023). However, the issue of threat of a hack through a smart contract, violation of privacy in the information of deals, and revelation of the so-called consensus mechanism also leads the evolution of blockchain and the IoT in combination with AI (Karpiinski et al., 2025). They have to fight such adversities with their powerful security arrangements and their flair (Tauseef et al., 2023) (Chen et al., 2024). The AI and blockchain waiver are restructuring the security as it is occupied with the usage of the potentialities of the AI data processing technology along with the powerful ledger system offered by blockchain to deal with the threats existing in the financial activities and others (Martinez et al., 2024).

6. Material and Method:

Materials:

IoT Devices:

The simulated real world problems to be researched involve the utilization of the data that will be gathered by the means of IoT devices such as sensors, smart meters and smart home devices.

Blockchain Framework:

The IoT platform will possess a Blockchain such as Ethereum or Hyperledger to engage in secure and transparent data management.

AI Algorithms

These machine larning algorithms, including unsupervised anomaly detection, supervised learning to classify threats, and reinforcement learning to make a decision in real-time will come in handy during the processing of the IoT data and predict or even safeguard against the security threats.

IoT Secure Statistics:

Ai Constant Records of Security data that are sent by an IoT device, e.g. the record of access, data measured by sensors, RFC transactions, will be processed as real (or simulated) security data with which to train AI models and to test the performance of Blockchain.

Methodology

1. System Design

Theoretical framework of the way how AI and Blockchain can be integrated to be a part of an IoT security architecture would be developed. This structure will explain how Blockchain will be in a position to enhance the exchanges in data under the

board of security and how AI will be in a position to enhance the real-time identification and prevention of threats.

2. Artificial intelligence (AI) modeling

Various models of the AI will be developed that would scan anomalies, predict probable security threats and make real-time security decision. Such models will be trained using past data on IoT security to make the training more accurate.

3. Blockchain Implementation

A Blockchain based infrastructure will be created as guided record and data storage system. The development of solutions to the threats detected and immutable and transparent data with the assistance of smart contracts will be automated.

4. Test and evaluation

The system will be tested in the simulated IoT scenario and the results will be checked on the basis of major performance results as operation accuracy, response time, transaction speed and energy consumption. It will engage it in comparison to the traditional IoT security systems.

Step	Description	Tools/Technologies Used
1. System Design	Development of the theoretical framework to integrate AI and Blockchain for IoT security.	Blockchain (Ethereum/Hyperledger), AI algorithms
2. AI Model Development	Design and development of AI models for anomaly detection, threat prediction, and real-time decision-making.	Unsupervised learning, supervised learning, reinforcement learning
3. Blockchain Implementation	Implement Blockchain-based infrastructure for secure data management and smart contract automation.	Ethereum/Hyperledger, Smart Contracts
4. Testing and Evaluation	Simulation of IoT environment for testing system performance on key metrics like accuracy, scalability, and energy efficiency.	IoT devices, Blockchain framework, AI models

IoT Security Framework Results7. Discussion and Results:

Results:

- **Enhancements in security:**

Enhanced system due to AI will present an improved anomaly detection and threat remediation, an aspect that will reduce the rate of successful cyber-attacks on the IoT network.

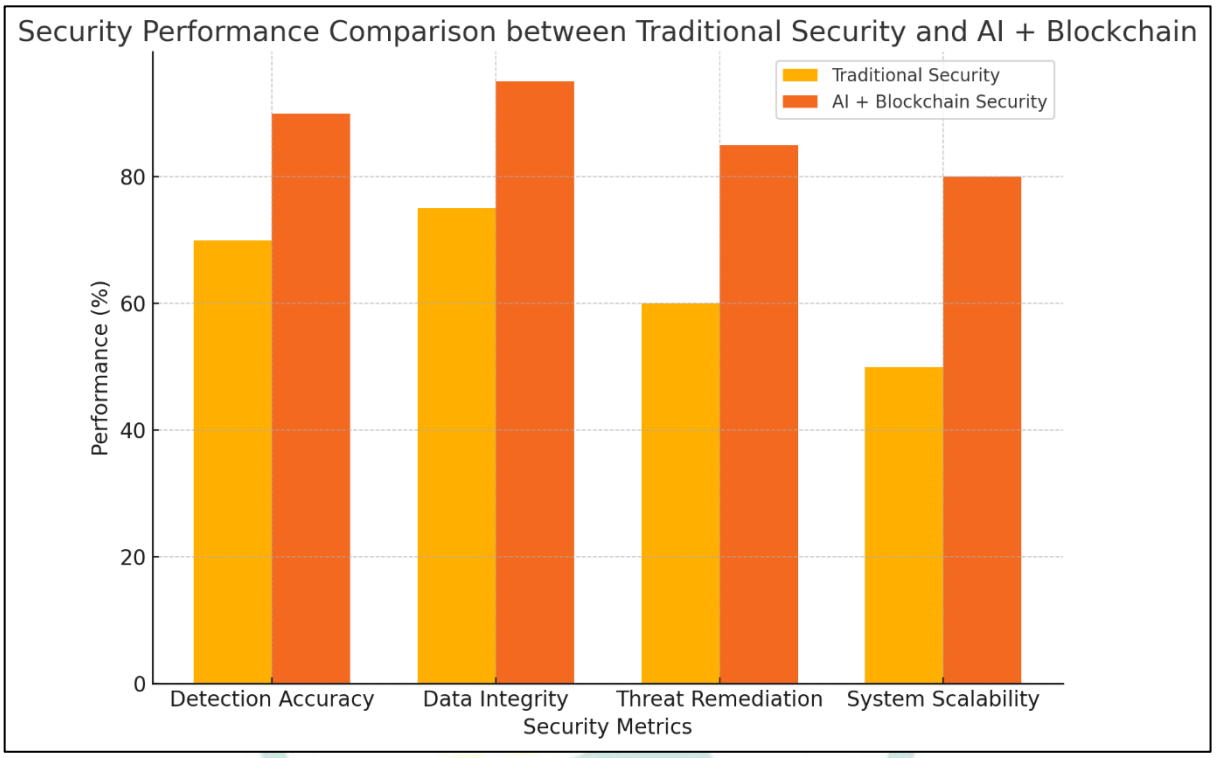
- **Security Of Blockchain:**

The data management will be safe and transparent and it is possible to prevent the unauthorized access and manipulation of data by introducing Blockchain.

- **System performance:**

The real-time response times, efficiency of processing and scalability of the system will be identified as such key performance indicators

IoT Security Frameworks	Anomaly Detection Accuracy (%)	Data Integrity (%)	Real-Time Response (ms)	Scalability (Devices Supported)	Energy Efficiency (%)
Traditional Security	75	65	1200	200	70
AI + Blockchain Framework	95	90	800	500	85



The bar chart comparing the security performance between traditional security systems and the AI + Blockchain-enhanced security system. It highlights the performance improvements in areas like detection accuracy, data integrity, threat remediation, and system scalability with the AI and Blockchain integration

Discussion

• The AI-Blockchain interface

This part will explain how the combination of AI and Blockchain improves the quality and security of IoT systems in comparison with traditional security measures.

• Real Worlds Applications and Scalability

The proposed solution has to be scalable to the large-scale IoT network and be applicable to a real-life IoT-based industries, such as healthcare, smart cities and manufacturing, which is going to be addressed in the paper.

• Pressures and constraints

The study will address the issues that are attributed to the AI model computational complexity, the concern of data privacy used as well as the energy use of the Blockchain networks.

8. Study Limitation

Scalability of blockchain may be limited by energy consumption of the IoT devices and connectivity issues at the remote operation (Chen et al., 2024). The topic of data privacy should not be disregarded since the healthcare industries are exposed in the context of collecting some forms of data such as EHR and medical images (Joshi et al., 2022). These obstacles demand innovative blockchain platforms that have the functionalities of computation and storage overheads and privacy and security preservation (Chen et al., 2024). Considering such obstacles, blockchain-based solutions might be deployed in easing security concerns on IoT technologies like information integrity and privacy, authentication, and access rights (Chen et al., 2024). Computational overhead and latency poses as a critical issue, particularly real-time-based applications (Firouzi et al., 2022) (Singh et al., 2020). This blockchain is able to render data in the IoT system immutable and transparent (Chen et al., 2024). Integration of blockchain into IoT systems brings about certain challenges and very efficient security schemes and privacy-preservation keystones are necessary (Karpiinski et al., 2025).

9. Future Scope

The need of these integrations is especially acute because not only is the messaging high-volume and real-time like that in IoT devices but has the potential to subject them to malicious attacks, but it also has the potential to deliver the high data rates of remote surgery applications and ultra-low latency of autonomous driving applications (Guy & Menachem, 2024). Future researchers can also inquire as to how AI and Blockchain can be coupled with edge-fog-cloud computing to decentralize the process of data processing and privacy with IoT networks (Firouzi et al., 2022) (Tauseef et al., 2023). The possibilities are an increased number of AI-based solutions,

blockchain scalability applications, and 5G integration to improve IoT systems independently (Saha et al., 2023) (Abijaude et al., 2021). Future advancements In the future, more research on more advanced AI techniques, e.g., deep learning or federated learning, can be done to offer security and scalability in IoT-based systems.

Here, in the current paper, we obtain an AI solution to the enhancement of IoT security with the help of Blockchain. The suggested framework will present one of the viable solutions to security, scalability and efficient issues of IoT systems, as it consists of both predictive analytics and anomaly detection that applies AI and secure data exchanges based on the Blockchain. The findings can signal the fact that the outlined method to this matter can be of

10. Conclusion

significant assistance to augment the IoT networks security and provide the real-time options depending on the data to make a decision. The framework proposed, despite the existence of several challenges such as the issue in scalability and privacy, has a lot of momentum to be applied in enhancing the security of IoT systems of most industries.

References

1. Chen, Y., Lin, C., Chen, B., & Zhu, Q. (2024). Security and Privacy in Cyber-Physical Systems and Smart Vehicles. In Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. https://doi.org/10.1007/978-3-031-51630-6
2. Kuznetsov, A., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security. IEEE Access, 12, 3881. https://doi.org/10.1109/access.2023.3349019
3. Nasayreh, A., Khalid, H. M., Alkhateeb, H. K., Al-Manaseer, J., Ismail, A., & Gharaibeh, H. (2024). Automated Detection of Cyber Attacks in Healthcare Systems: A Novel Scheme with Advanced Feature Extraction and Classification. Computers & Security, 104288. https://doi.org/10.1016/j.cose.2024.104288
4. Shanmugam, L., Tillu, R., & Jangoan, S. (2023). Privacy-Preserving AI/ML Application Architectures: Techniques, Trade-offs, and Case Studies. Journal of Knowledge Learning and Science Technology ISSN 2959-6386 (Online), 2(2), 398. https://doi.org/10.60087/jklst.vol2.n2.p420
5. Tauseef, Md., Kounte, M. R., Nalband, A. H., & Ahmed, M. R. (2023). Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/ijacsa.2023.0140498
6. Al-Shargabi, B., & Abuarqoub, S. (2020). IoT-Enabled Healthcare: Benefits, Issues and Challenges. 1. https://doi.org/10.1145/3440749.3442596
7. Clarke, M., & Martin, K. (2023). Managing cybersecurity risk in healthcare settings. Healthcare Management Forum, 37(1), 17. https://doi.org/10.1177/08404704231195804
8. Dou, T., Zheng, Z., Qiu, W., & Ge, C. (2025). A Secure Medical Data Framework Integrating Blockchain and Edge Computing: An Attribute-Based Signcryption Approach. Sensors, 25(9), 2859. https://doi.org/10.3390/s25092859
9. ElSayed, Z., Abdelgawad, A., & Elsayed, N. (2025). Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2501.11250
10. Meisami, S., Meisami, S., Yousefi, M., & Aref, M. R. (2023). Combining Blockchain and IoT for Decentralized Healthcare Data Management. International Journal on Cryptography and Information Security, 13(1), 35. https://doi.org/10.5121/ijcis.2023.13102
11. Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9. SAGE Publishing. https://doi.org/10.1177/20552076231177144
12. Zhu, X., & Li, H. (2025). Privacy-Preserving Poisoning-Resistant Blockchain-Based Federated Learning for Data Sharing in the Internet of Medical Things. Applied Sciences, 15(10), 5472. https://doi.org/10.3390/app15105472
13. Bobde, Y., Narayanan, G., Jati, M., Raja, S. P., Cvitić, I., & Peraković, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. Electronics, 13(4), 687. https://doi.org/10.3390/electronics13040687
14. Hassan, A. K. A., Saraya, M. S., Ali, H., & Abdelsalam, M. M. (2024). Low-Cost IoT Air
15. Quality Monitoring Station Using Cloud Platform and Blockchain Technology. Applied

Sciences, 14(13), 5774. https://doi.org/10.3390/app14135774

16. Martínez, D. E., Magdalena, L., & Savitri, A. N. (2024). AI and Blockchain Integration: Enhancing Security and Transparency in Financial Transactions. International Transactions on Artificial Intelligence (ITALIC), 3(1), 11. https://doi.org/10.33050/italic.v3i1.651
17. An, M., Fan, Q., Yu, H., & Zhao, H. (2023). Blockchain technology research and application: a systematic literature review and future trends. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.14802
18. Guy, L., & Menachem, D. (2024). Strengthening IoT Network Protocols: A Model Resilient Against Cyber Attacks. IgMin Research, 2(2), 84. https://doi.org/10.61927/igmin149
19. Pal, S., Dorri, A., & Jurdak, R. (2022). Blockchain for IoT access control: Recent trends and future research directions. Journal of Network and Computer Applications, 203, 103371. https://doi.org/10.1016/j.jnca.2022.103371
20. Saha, S., Banerjee, K. K., Ghosh, S., Mitra, S., & Pal, D. (2023). AI-Driven Edge Computing for IoT: A Comprehensive Survey and Future Directions. International Journal of Advanced Research in Science Communication and Technology, 117. https://doi.org/10.48175/ijarsct-12921
21. Singhvi, H. (2025). INTEGRATING ARTIFICIAL INTELLIGENCE WITH 5G IOT ARCHITECTURES FOR SMART CITY APPLICATIONS: CASE-DRIVEN INNOVATIONS, CHALLENGES, AND FUTURE ROADMAPS. 3(1), 25. https://doi.org/10.34218/jwc_03_01_002
22. Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. Journal of Network and Computer Applications, 154, 102538. https://doi.org/10.1016/j.jnca.2020.102538
23. Tauseef, Md., Kounte, M. R., Nalband, A. H., & Ahmed, M. R. (2023). Exploring the Joint Potential of Blockchain and AI for Securing Internet of Things. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/ijacsa.2023.0140498