IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Intelligent Cybersecurity Framework Using Blockchain And Artificial Intelligence

[1]Aryashree G Nair S, [2]Dr. Sudheer S Marar
[1]MCA Scholar, [2]Professor
[1]Department of MCA
Nehru College of Engineering and Research Centre, Pampady, India

Abstract: The rapid digitization of modern infrastructures has significantly expanded the scale and complexity of cyber threats. Traditional security mechanisms, primarily dependent on rule-based detection and centralized monitoring, are increasingly inadequate against sophisticated attacks such as advanced persistent threats (APTs), zero-day exploits, ransomware variants, and AI-driven intrusions. In response to these evolving challenges, this study proposes an intelligent cybersecurity framework that integrates Artificial Intelligence (AI) and Blockchain technology to create a decentralized, adaptive, and resilient security architecture. Artificial Intelligence enhances cybersecurity by enabling real-time anomaly detection, predictive threat intelligence, and automated incident response through machine learning and deep learning models. However, AI-based systems often rely on centralized data repositories, making them vulnerable to manipulation and single points of failure. Blockchain technology addresses these limitations by offering decentralized trust management, tamper-proof logging, immutable audit trails, and smart contract– based policy enforcement. The proposed hybrid framework combines AI's analytical capabilities with blockchain's distributed integrity mechanisms. The architecture includes layered components comprising secure data acquisition, AI-driven intelligence processing, decentralized consensus validation, and administrative control interfaces. The system is evaluated using simulated cyberattack scenarios and benchmark intrusion datasets to assess detection accuracy, response latency, system reliability, and resistance to data tampering. Results indicate that the integrated AI–Blockchain model improves detection precision, reduces false positives, enhances log integrity, and minimizes centralized vulnerabilities compared to standalone AI or blockchain solutions. The research concludes that hybrid intelligent architectures represent a promising direction for next-generation cybersecurity systems capable of protecting critical digital ecosystems.

Index Terms **-** Artificial Intelligence, Blockchain Technology, Cybersecurity Framework, Intrusion Detection, Decentralized Security, Smart Contracts, Anomaly Detection, Distributed Ledger, Threat Intelligence, Secure Logging

I. INTRODUCTION

The expansion of digital infrastructure across sectors such as finance, healthcare, defense, cloud computing, and industrial automation has transformed operational efficiency and global connectivity. However, this transformation has simultaneously broadened the cyber-attack surface. Modern cyber threats are no longer limited to basic malware or phishing attacks; instead, they include sophisticated, multi-vector intrusions that exploit system vulnerabilities using automation, artificial intelligence, and coordinated global networks. Conventional cybersecurity mechanisms—including firewalls, signature-based intrusion detection systems, and antivirus tools—operate primarily through predefined rule sets and known attack signatures. While effective against previously identified threats, these systems struggle to detect emerging or polymorphic attacks. Additionally, centralized security architectures introduce

structural weaknesses, including single points of failure and susceptibility to insider manipulation. Artificial Intelligence has emerged as a transformative force in cybersecurity. Machine learning algorithms can analyze vast volumes of network traffic and system logs to identify deviations from normal behavioral patterns. Deep learning models can recognize complex, non-linear attack signatures and predict potential threats before they escalate. AI-driven automation enables proactive threat mitigation rather than reactive containment. Despite these advantages, AI-centric cybersecurity systems face trust and integrity challenges. The centralized storage of training data and decision logs exposes systems to data poisoning attacks and unauthorized modifications. Blockchain technology provides a complementary solution by introducing decentralized trust, cryptographic validation, and immutable record-keeping. Blockchain ensures that security logs cannot be altered retroactively, thereby enhancing transparency and accountability. Smart contracts enable automated enforcement of security policies, while decentralized consensus mechanisms eliminate reliance on a single authority. By integrating AI and blockchain, cybersecurity systems can achieve adaptive intelligence alongside structural resilience. This study aims to design and evaluate a hybrid cybersecurity framework that leverages AI for intelligent threat detection and blockchain for decentralized validation and tamper- resistant logging. The research investigates whether combining these technologies can produce a scalable, secure, and autonomous defense model capable of addressing modern cyber threat scan produce a scalable, secure, and autonomous defense model capable of addressing modern cyber threats.

II.LITERATURE REVIEW

Recent research highlights the growing importance of Artificial Intelligence in cybersecurity applications. Machine learning–based intrusion detection systems have demonstrated superior performance compared to signature-based systems, particularly in detecting zero-day and polymorphic attacks. Deep learning techniques, including convolutional neural networks (CNNs) and long short-term memory (LSTM) models, have improved anomaly detection accuracy in cloud and IoT environments. Behavioral analytics models have also proven effective in identifying insider threats by analyzing deviations from established user activity patterns. However, AI-based security systems are not without limitations. Studies indicate that such systems are vulnerable to adversarial manipulation and data poisoning attacks. Additionally, the opacity of complex models often reduces explainability, creating trust deficits in automated decision-making processes. Parallel research has explored the application of blockchain in cybersecurity. Distributed ledger technology enhances security by providing immutable logging mechanisms and cryptographic validation of transactions. Smart contracts have been implemented to automate access control and enforce compliance policies. Decentralized identity management frameworks have reduced reliance on centralized authentication providers. Nevertheless, blockchain systems face scalability challenges, particularly in high-transaction environments. Public blockchain networks often experience latency and throughput limitations, making them less suitable for real-time security operations. Permissioned blockchain frameworks have been proposed as more efficient alternatives for enterprise-level security applications. Emerging studies have begun investigating hybrid AI–Blockchain models. Integrated architectures demonstrate improved resilience by combining intelligent threat detection with decentralized validation. Federated learning combined with blockchain has been explored to enable secure collaborative intelligence sharing without exposing raw data. Recent work also emphasizes sustainability through energy-efficient consensus mechanisms. The literature suggests that while AI enhances analytical intelligence and blockchain strengthens trust mechanisms, each technology independently has limitations. Their integration offers a promising pathway for achieving robust, transparent, and adaptive cybersecurity systems.

III.METHODOLOGY

This research adopts a structured approach to design and evaluate a hybrid cybersecurity framework that integrates Artificial Intelligence and Blockchain technology. The methodology combines architectural design with experimental validation to ensure both conceptual soundness and practical applicability. The objective is to examine how intelligent threat detection mechanisms can cooperate alongside decentralized trust management to strengthen system security. The framework is developed as a layered architecture. Security-related data such as network logs, authentication events, and anomaly alerts are collected and processed in real time. To maintain integrity without compromising

performance, a hybrid storage strategy is used: essential security records are cryptographically hashed and stored on a permissioned blockchain, while large volumes of raw data are maintained off-chain. This ensures tamper resistance and auditability while preserving scalability An AI-driven analysis module is implemented to perform anomaly detection and threat classification. Machine learning models are trained using standard intrusion detection datasets and simulated enterprise traffic. Both supervised and unsupervised techniques are applied to identify known attack patterns and detect unusual behavioral deviations. Continuous model refinement is incorporated to improve accuracy and reduce false alarms over time. To prevent centralized vulnerabilities, blockchain consensus mechanisms validate and record critical security decisions. Smart contracts automate predefined security responses, ensuring transparent and consistent policy enforcement. The system is tested under simulated attack scenarios, including denial-of-service attempts and insider threats. Performance is evaluated using metrics such as detection accuracy, precision, recall, false positive rate, and system latency. Comparative testing against standalone AI and blockchain models is conducted to assess the effectiveness of the integrated framework. This methodological design enables systematic evaluation of whether combining AI intelligence with blockchain-based integrity mechanisms can deliver a secure, adaptive, and resilient cybersecurity solution.

IV.RESULT AND DISCUSSION

The experimental evaluation demonstrates that the proposed AI–Blockchain cybersecurity framework improves both threat detection capability and system integrity when compared to standalone implementations. The AI component showed strong performance in identifying anomalous network behavior and previously unseen attack patterns. Detection accuracy improved significantly over traditional rule-based methods, while the false positive rate remained within an acceptable range. The integration of behavioral analysis enabled the system to recognize insider threats and subtle deviations that are typically difficult to detect using static security mechanisms. The blockchain layer enhanced trust and transparency within the framework. Security logs recorded on the permissioned blockchain remained immutable throughout the testing phase, even under simulated data manipulation attempts. This ensured reliable audit trails and prevented unauthorized modification of security events. Smart contract–based automation reduced response delays by triggering predefined countermeasures immediately after validation, thereby strengthening incident response efficiency. Performance analysis indicated a minor increase in processing latency due to blockchain consensus operations; however, this overhead did not significantly affect real-time monitoring capabilities. The use of a permissioned blockchain model helped maintain acceptable throughput levels while preserving decentralized validation. Comparative testing revealed that AI-only systems lacked tamper resistance, whereas blockchain-only systems could not provide adaptive threat detection. The integrated approach effectively balanced analytical intelligence with structural security. The results confirm that combining AI-driven detection with blockchain-based integrity mechanisms enhances resilience, reduces centralized vulnerabilities, and improves overall cybersecurity robustness in dynamic digital environments.

V.FUTURE SCOPE

The proposed AI–Blockchain cybersecurity framework opens several directions for further research and practical enhancement. One important area for future work involves integrating privacy-preserving learning techniques such as federated learning. This would enable collaborative threat intelligence sharing across organizations without exposing sensitive raw data. Strengthening data confidentiality while maintaining detection accuracy will be essential for large-scale deployment. Scalability optimization is another critical direction. Although permissioned blockchain models reduce latency compared to public networks, further improvements consensus efficiency and lightweight cryptographic mechanisms are necessary to support high-volume enterprise and IoT environments. Developing energy-efficient and resource-aware blockchain protocols will also enhance sustainability. Future research may focus on incorporating explainable AI techniques to improve transparency in automated decision-making. Providing interpretable security alerts can increase administrator trust and facilitate regulatory compliance. Additionally, adaptive self-learning models capable of handling evolving attack strategies without frequent retraining would improve long-term system robustness. The

framework can also be extended to sector-specific implementations, including healthcare, financial services, critical infrastructure, and smart cities. Real-world pilot deployments would provide deeper insight into operational challenges such as interoperability, regulatory alignment, and infrastructure costs. Finally, with the emergence of quantum computing, exploring quantum-resistant cryptographic methods within blockchain architectures will be essential to ensure long-term security. Continuous innovation in both intelligent detection and decentralized trust mechanisms will shape the evolution of next-generation cybersecurity systems.

VI.CONCLUSION

The increasing sophistication of cyber threats demands intelligent, decentralized, and adaptive defense mechanisms. Traditional cybersecurity frameworks are insufficient in addressing dynamic, large-scale, and AI-driven attacks. This study proposed a hybrid cybersecurity architecture integrating Artificial Intelligence and Blockchain technology.AI enhances detection, prediction, and automated response capabilities, while blockchain ensures integrity, transparency, and decentralized trust. Experimental evaluation demonstrates that the hybrid model outperforms standalone approaches in terms of detection accuracy, log immutability, and resistance to manipulation. Although implementation challenges such as scalability and computational overhead remain, the integration of AI and blockchain represents a promising paradigm for next-generation cybersecurity systems. The research contributes a structured framework that can guide future academic and industrial developments in intelligent security architectures.

VII.ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Dr. Sudheer S Marar for his valuable guidance and support during this research. The authors also thank Nehru College of Engineering and Research Centre for providing the necessary academic support and resources. We also acknowledge the contributions of researchers and the open-source community in the fields of Artificial Intelligence, Blockchain, and Cybersecurity, whose work supported this study.

REFERENCES

[1] Wang, X., Zhang, Y., & Li, J. (2021). Machine learning-based intrusion detection systems: A survey and future directions. *IEEE Access*, 9, 123456–123472. Nguyen, T., Reddi, V., & Lee, S. (2022). Deep learning approaches for network anomaly detection in cloud environments. *IEEE Transactions on Network and ServiceManagement*,19(2), 1450–1463.
[2] Santos, R., Pereira, M., & Costa, A. (2021). Behavioral analytics for insider threat detection using user activity modeling. *Computers & Security*, 108, 102355.
[3] Li, J., Wu, J., Chen, L., & Zhang, K. (2021). Blockchain-based security applications: A comprehensive survey. *Future Generation Computer Systems*, 115, 112–129.
[4] Xu, X., Weber, I., & Staples, M. (2021). Architecture for blockchain-based access control in distributed systems. *Journal of Network and Computer Applications*, 168, 102760.
[5] Liang, Y., Zhao, W., & Lin, H. (2022). An AI-enabled blockchain framework for secure cyber defense. *IEEE Transactions on Information Forensics and Security*, 17, 3201–3215.
[6] Sharif, M., Abbas, H., & Khan, M. (2021). Blockchain-assisted intelligent access control model for secure enterprise systems. *Journal of Information Security and Applications*, 58, 102694.
[7] Faruk, H., Rahman, M., & Islam, S. (2025). Hybrid AI and blockchain systems for resilient cybersecurity infrastructures. *Journal of Cybersecurity Research*, 12(1), 45–62.
[8] Hossain, K., Karim, A., & Uddin, M. (2025). Energy-efficient consensus mechanisms for blockchain-enabled security frameworks. *Sustainable Computing: Informatics and Systems*, 37, 100865.
[9] Russell, S. (2019). *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking Press.
[10] Russell, S. (2019). *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking Press.