A Comprehensive Review of Blockchain-Based Intrusion Detection Systems for IoT Networks

Sandhya Jaiswal
MTech Scholar,CSE Department
NRI Bhopal
Jaissandhya721@gmail.com

Prof. Anurag Shrivastava
Asso. Professor, CSE Department
NRI Bhopal
anurag.shri08@gmail.com

***Abstract*:** The rapid growth of Internet of Things (IoT) networks has increased security vulnerabilities due to their distributed, resource-constrained, and heterogeneous nature. Traditional intrusion detection systems (IDS) often face limitations related to scalability, data integrity, and centralized trust. This review presents a comprehensive analysis of blockchain-based intrusion detection systems for IoT networks, highlighting how blockchain technology enhances security through decentralization, immutability, and transparent data sharing. Existing studies integrating blockchain with machine learning and deep learning–based IDS are examined, along with commonly used architectures, consensus mechanisms, and performance metrics. The review also discusses key challenges such as computational overhead, latency, and energy consumption. Finally, open research issues and future directions are identified to support the development of secure, efficient, and scalable blockchain-enabled IDS solutions for IoT environments.

Keywords*— *Blockchain, Intrusion Detection System, Internet of Things, Network Security, Machine Learning, Decentralization, Smart Contracts

I. INTRODUCTION

The rapid advancement of the Internet of Things (IoT) has transformed modern digital ecosystems by enabling seamless connectivity among billions of smart devices across diverse domains such as healthcare, smart cities, industrial automation, and intelligent transportation systems. Despite these benefits, IoT networks are highly vulnerable to cyberattacks due to their open communication environments, heterogeneous architectures, limited computational resources, and lack of robust security mechanisms. Traditional security solutions, particularly centralized intrusion detection systems (IDS), often struggle to provide effective protection in IoT environments because of scalability issues, single points of failure, and challenges related to trust and data integrity. Intrusion Detection Systems play a critical role in identifying malicious activities, unauthorized access, and abnormal network behavior. However, conventional IDS approaches rely heavily on centralized data collection and analysis, making them susceptible to tampering, data manipulation, and delayed response times. Moreover, the increasing sophistication of cyberattacks necessitates collaborative and trustworthy detection mechanisms capable of operating efficiently in distributed IoT networks.

Blockchain technology has emerged as a promising solution to address these limitations by introducing decentralization, immutability, transparency, and trustless communication. By leveraging distributed ledger technology, blockchain-based IDS can securely store intrusion logs, share threat intelligence among IoT nodes, and prevent unauthorized modifications of security data. Smart contracts further enhance automation by enabling real-time alert generation, access control, and coordinated response actions without relying on a centralized authority. Recent research has explored the integration of blockchain with machine learning and deep learning techniques to improve intrusion detection accuracy while ensuring secure and verifiable data exchange. Although blockchain-based IDS frameworks demonstrate significant potential, challenges such as computational overhead, latency, energy consumption, and scalability remain critical concerns for resource-constrained IoT devices. Therefore, a comprehensive review of existing blockchain-enabled IDS approaches is essential to understand current advancements, architectural designs, performance trade-offs, and open research challenges. This review aims to systematically analyze blockchain-based intrusion detection systems in IoT networks, highlighting their benefits, limitations, and future research directions toward building secure, efficient, and scalable IoT security solutions.

Furthermore, the integration of blockchain with intrusion detection systems offers enhanced resilience against data tampering and insider attacks by ensuring secure and verifiable storage of security events. Distributed consensus mechanisms enable collaborative threat detection across multiple IoT nodes without relying on a centralized authority. This decentralized approach improves trust, fault tolerance, and transparency in IoT security management. However, selecting suitable blockchain platforms, consensus algorithms, and lightweight cryptographic techniques remains a challenge due to the limited computational and energy resources of IoT devices. Addressing these constraints while maintaining high detection accuracy is critical for real-world deployment. Consequently, ongoing research focuses on optimizing blockchain-enabled IDS architectures to balance security, efficiency, and scalability in dynamic IoT environments.

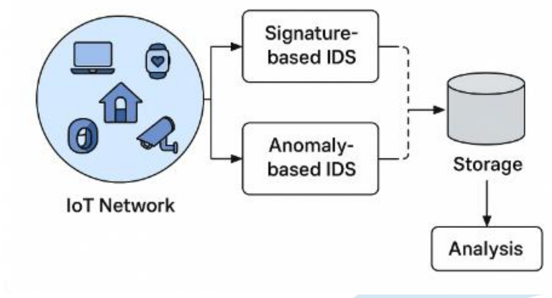

Figure 1. Intrusion Detection in IoT

II. LITRETURE REVIEW

The literature reveals extensive research on intrusion detection systems for IoT networks, focusing on signature-based, anomaly-based, and hybrid approaches. Traditional IDS methods often face limitations related to scalability, centralized trust, and vulnerability to single points of failure. Recent studies highlight the integration of machine learning and deep learning techniques to improve detection accuracy and adaptability to evolving attacks. Blockchain-based IDS frameworks have been proposed to enhance data integrity, decentralization, and secure information sharing among IoT nodes. Despite promising results, challenges such as computational overhead, latency, and real-world deployment constraints remain open research issues.

Author [1] proposes a blockchain-based hybrid intrusion detection system (BC-HyIDS) for secure signature exchange in distributed IoT networks. The framework integrates signature-based and anomaly-based detection with blockchain to enhance data security and trust. Implemented using Hyperledger Fabric v2.0 and Hyperledger Sawtooth, the system employs cryptographic techniques for secure data storage. Experimental results show improved performance in terms of accuracy, detection rate, and reduced false alarm rate, demonstrating the effectiveness of blockchain integration in intrusion detection systems.

This paper Author [2] focuses on conducting a Systematic Literature Review (SLR) on Blockchain-based Intrusion Detection/Prevention Systems in IoT Networks. We reviewed several relevant blockchain-based IDS and IPS proposed for IoT networks and their mechanisms. The most recent research articles, published between 2017 and 2022, were selected from several data.

In this work Authors [3] presents a hybrid intrusion detection approach that integrates machine learning with blockchain to detect cyber threats in resource-constrained IoT environments. The proposed hybrid decision tree (HIDT) model achieves high attack detection accuracy on benchmark datasets while maintaining low false positive and false negative rates. The system enables rapid identification of malicious nodes, reducing network delay and routing overhead. Experimental results demonstrate improved throughput, scalability, and robustness, highlighting the effectiveness of blockchain-enabled intelligent intrusion detection for securing IoT and cyber-physical networks.

Authors [4] addressed the security challenges in Internet of Medical Things (IoMT) networks, highlighting the limitations of traditional security mechanisms in highly dynamic and interconnected environments. The study emphasized that centralized machine learning–based intrusion detection systems suffer from privacy risks and single points of failure. To overcome these issues, the authors explored federated learning to enable privacy-preserving intrusion detection through local model training on end devices. Furthermore, blockchain technology was incorporated to ensure secure and trustworthy collaboration among distributed nodes. The proposed approach demonstrated high intrusion detection accuracy while effectively preserving data privacy in IoMT networks.

Authors [5] proposed a blockchain-based collaborative intrusion detection framework to address the increasing complexity of modern cyber threats. The study highlighted the importance of collaborative intrusion detection systems in improving threat detection and information sharing. To reduce alert collisions during data exchange, an efficient leader node selection mechanism was introduced. Unlike traditional node-level detection approaches, the framework employed an ensemble learning–based collaborative detection strategy, resulting in improved detection precision. Experimental evaluation using benchmark datasets demonstrated that the proposed framework outperformed conventional intrusion detection systems, confirming its effectiveness in enhancing cybersecurity defenses.

Authors [6] proposed a blockchain-enabled intrusion detection model to enhance the security of Internet of Things (IoT) networks by ensuring data integrity, decentralization, and tamper-proof logging. The study integrated blockchain consensus mechanisms with federated-style local training, lightweight cryptography, and SHAP-based explainability to improve both security and interpretability. The proposed framework combined blockchain technology with explainable artificial intelligence to enable transparent and real-time detection of various cyberattacks, including DoS, DDoS, scanning, injection, and backdoor attacks. Performance evaluations demonstrated that the blockchain-enabled IDS outperformed existing approaches, offering a robust, flexible, and interpretable cybersecurity solution for modern IoT environments.

III. FINDINGS OF THE SURVEY

This survey provides a comprehensive analysis of recent advancements in intrusion detection systems (IDS) for Internet of Things (IoT) and Internet of Medical Things (IoMT) networks, with a particular focus on blockchain-enabled and machine learning based approaches. The findings reveal that traditional IDS techniques, including signature-based and rule-based methods, are increasingly insufficient for modern IoT environments due to their centralized architectures, limited scalability, and vulnerability to single points of failure. As IoT networks grow in size and complexity, these limitations significantly reduce detection efficiency and system reliability.

Machine learning–based IDS models have shown notable improvements in detecting complex and previously unseen cyberattacks by learning patterns from network traffic and system behavior. Algorithms such as Random Forest, XGBoost, LightGBM, convolutional neural networks (CNNs), and recurrent neural networks (RNNs) consistently outperform traditional methods in terms of detection accuracy and adaptability. However, the survey identifies privacy risks and trust issues associated with centralized ML models, especially when sensitive healthcare or personal data are involved.

To address these concerns, federated learning has emerged as an effective solution by enabling decentralized model training directly on IoT devices without sharing raw data. The survey findings indicate that federated learning–based IDS frameworks maintain competitive detection performance while significantly enhancing data privacy. Furthermore, the integration of blockchain technology strengthens these systems by ensuring secure data sharing, immutable logging, decentralized trust, and resistance to data tampering. Blockchain-based IDS frameworks also facilitate collaborative intrusion detection by enabling reliable exchange of alerts and threat intelligence among distributed nodes.

Explainable artificial intelligence techniques, particularly SHAP-based analysis, are increasingly incorporated to improve transparency and interpretability of IDS decisions. The survey highlights that explainable models enhance clinical and operational trust by clearly identifying influential features such as traffic patterns, device behavior, and system-level indicators. Additionally, blockchain-enabled IDS systems demonstrate reduced false alarm rates, improved detection precision, and better resilience against insider and adversarial attacks.

Despite these advancements, the survey identifies several challenges, including computational overhead, latency, energy consumption, and the need for lightweight consensus mechanisms suitable for resource-constrained IoT devices. Moreover, many existing studies rely on benchmark datasets and lack real-world deployment and external validation. Overall, the findings confirm that blockchain-integrated, machine learning–based IDS frameworks represent a robust and promising direction for securing IoT networks, while emphasizing the need for scalable architectures, explainable models, and real-world evaluation to support practical adoption.

CONCLUSION

This survey concludes that blockchain-enabled intrusion detection systems combined with machine learning and federated learning offer a powerful solution for securing IoT and IoMT networks. These approaches effectively overcome the limitations of traditional centralized IDS by enhancing data integrity, decentralization, privacy, and trust. The integration of explainable artificial intelligence further improves transparency and reliability in intrusion detection decisions. Despite promising performance in terms of accuracy and reduced false alarms, challenges related to scalability, computational overhead, and real-world deployment remain. Future research should focus on lightweight blockchain architectures, energy-efficient learning models, and large-scale real-world validation to ensure practical, secure, and scalable intrusion detection solutions for modern connected environments.

REFERENCES

[1] S. R. Khonde et. al. "Hybrid intrusion detection system using blockchain framework" Khonde and Ulagamuthalvi J Wireless Com Network (2022) 2022:58 https://doi.org/10.1186/s13638-022-02089-4

[2]Khawla Shalabi et. al "A Blockchain-based Intrusion Detection/Prevention" ScienceDirect, Procedia Computer Science 236 (2024) 410–419

[3] Shailendra Mishra et. al. "Blockchain and Machine Learning-Based Hybrid IDS to Protect Smart Networks and Preserve Privacy" https://doi.org/10.3390/electronics12163524

[4] Khadija Begum et. al. "BFLIDS: Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks" Blockchain-Driven Federated Learning for Intrusion Detection in IoMT Networks. Sensors 2024 https://doi.org/10.3390/ s24144591, MPDI 2024

[5] Jiachen Huang et. al. "Optimization Scheme of Collaborative Intrusion Detection System Based on Blockchain Technology" Electronics 2025, 14, 261 https://doi.org/10.3390/electronics14020261

[6] Atul Kumar1, et. al. "Secure blockchain based intrusion detection for IoT networks" Kumar et al. Discover Computing (2025) 28:226, https://doi.org/10.1007/s10791-025-09754-4 Discover 2025

[7] Shailender Kumar Vats et. al. "Securing Distributed Blockchain Ledgers: An Intrusion Detection System Powered by Advanced Smart Contracts for Enhanced Cloud-Based Big Data Storage" International Journal of Intelligent Systems and Applications in Engineering IJISAE, 2024, 12(3), 901–909

[8] Chakir O, Sadqi Y, Abdellaoui Alaoui EA. An explainable machine learning-based web attack detection system for industrial IoT web application security. Inform Secur J Glob Perspect. 2024; 1–27.

[9] Awad M, Fraihat S, Salameh K, Redhaei A, A. Examining the suitability of netflow features in detecting IoT network intrusions. Sensors. 2022;22(16):6164.

[10] Swain PK, Pattnaik LM, Satpathy S. IoT applications and cyber threats: mitigation strategies for a secure future. In: Explainable IoT applications: A demystification. Cham: Springer Nature Switzerland; 2025. p. 403–28.

[11] Abed-alguni BH, Alzboun BM, Alawad NA. BOC-PDO: an intrusion detection model using binary opposition cellular prairie
dog optimization algorithm. Cluster Comput. 2024;27(10):14417–49.

[12] Doriguzzi-Corin R, Knob LAD, Mendozzi L, Siracusa D, Savi M. Introducing packet-level analysis in programmable data
planes to advance network intrusion detection. Comput Networks. 2024;239:110162.

[13] Batchu RK, Bikku T, Thota S, Seetha H, Ayoade AA. A novel optimization-driven deep learning model for the detection of
DDoS attacks. Sci Rep. 2024;14(1):28024.

[14] Le TTH, Kim H, Kang H, Kim H. Classification and explanation for intrusion detection system based on ensemble trees and SHAP method. Sensors. 2022;22(3):1154.

[15] Muna RK, Hossain MI, Alam MGR, Hassan MM, Ianni M, Fortino G. Demystifying machine learning models of massive IoT
attack detection with explainable AI for sustainable and secure future smart cities. Internet of Things. 2023;24:100919.

[16] Fraihat S, Makhadmeh S, Awad M, Al-Betar MA, Al-Redhaei A. Intrusion detection system for large-scale IoT netflow networks
using machine learning with modified arithmetic optimization algorithm. Internet of Things. 2023;22:100819.