**Increased Accuracy in Blockchain-Based Intrusion Detection and Prevention System**

Aliyu Ahmed A1,2, Jinshuo Liu1, Ezekia Gilliard1

1 *School of Cyber Science and Engineering, Wuhan University, Wuhan, China, 430000*

2 *Department of computer Science, Faculty of Computing, Kaduna State University, Kaduna, Nigeria, 800283*

Email: ahmed.aliyu@kasu.edu.ng.

Intrusion Detection and Prevention (IDPS) is a critical cybersecurity task that involves monitoring network traffic for malicious activity and taking appropriate action to stop it. However, insufficient training data or improperly chosen thresholds often limit the accuracy of such systems, resulting in high false positive rates. To improve the accuracy of an IDPS, blockchain technology can be used. Blockchain technology provides a secure, decentralized, immutable ledger that can track suspicious activity over time and identify intrusions globally. Security teams can use blockchain technology to create immutable records of suspicious activity, give users visibility into the system, and improve the accuracy of intrusion detection systems. In this paper, we propose a novel methodology to improve the accuracy of blockchain-based intrusion detection and prevention systems, which is based on combining different intrusion detection algorithms and using a blockchain-integrated architecture. Our experimental results show that the proposed system significantly increases the accuracy while reducing the false positive rate, opening up new opportunities for the development of highly accurate networks.

*Introduction*

Blockchain technology has drawn more attention in recent years due to its potential applications in various industries, including finance, healthcare, and cybersecurity. In particular, developing IDPS based on blockchain technology could significantly improve the accuracy of intrusion detection while lowering false alarms and improving scalability [1]. As a result, this research aims to present a novel methodology in this paper that will improve the accuracy of blockchain-based IDPS. The paper outlines a technological approach that uses a blockchain-integrated architecture to improve the system's scalability and accuracy while combining multiple IDPS algorithms to detect intrusion attempts. Multiple datasets are used to test the proposed methodology, and we report how accurate it is compared to current systems.

*Background and Related Work*

Critical cybersecurity tasks include intrusion detection and prevention, which involve monitoring network traffic for malicious activity and taking appropriate action to stop it. To identify signs of an attack, IDPS typically combine rules-based monitoring, machine learning (ML) models, anomaly detection, and other techniques [2]. However, insufficient training data or improperly chosen thresholds frequently limit the accuracy of such systems, leading to high false positive rates.

An effective solution for improving an IDPS accuracy is to use blockchain technology. Blockchain offers a secure, decentralized, immutable ledger that can track suspicious activity over time and identify intrusions globally [3]. This blockchain technology can track suspicious patterns in network traffic and more effectively detect intrusions. Additionally, security teams can use blockchain technology to create immutable records of suspicious activity, which will help them better recognize and respond to threats [4]. Blockchain technology can also give users visibility into the system, which helps security teams better understand the activities on the system's network [5]. Last, blockchain technology has enormous potential to improve intrusion detection systems' precision.

Various researchers have proposed blockchain-based IDPS that make use of a variety of techniques, including node clustering for storing and sharing distributed information, support vector machine (SVM) classifiers for quick and accurate detection of network intrusions, anomaly detection based on big data technology, and more. The alert messages based on these systems are subject to bias and human errors, which reduces their accuracy and responsiveness [6]. Despite these improvements, these systems still need help with false positives and scalability. Furthermore, because these systems are distributed, identifying and stopping malicious activity is more challenging because it could originate from any node and go undetected [7]. This further reduces the general responsiveness and accuracy of such systems. A more reliable and accurate detection system must be established to detect and stop malicious activity effectively.

*Proposed Research Methodology*

This section suggests a novel technique for improved IDPS accuracy in blockchain-based systems. The strategy is based on the fusion principle, in which different IDPS algorithms are combined using weighted votes to determine the outcome. The proposed system integrates various algorithms into a single blockchain-based architecture, making it highly monitored and impenetrable. The system also uses artificial intelligence (AI) technology to enhance accuracy and scalability. Node-level IDPS, distributed blockchain-based IDPS, machine learning-based IDPS, and artificial intelligence-based IDPS are the four main parts of the proposed system.

Node-Level IDPS

At the node level, IDPS are crucial for network security and safety. It is in charge of monitoring the activity at the nodes, identifying potential anomalies, and sending out alerts to ensure the proper course of action is taken [8]. Typically, it employs anomalies-based detection for unknown threats or signature-based detection for known attacks [10]. In addition, malicious nodes can be found using the node-level IDPS by examining their communication patterns [9]. This feature may be very helpful in protecting the network's integrity and preventing malicious users. As a result, a reliable node-level IDPS is a crucial part of a strong cybersecurity system.

Distributed Blockchain-Based IDPS

Network log data distribution and real-time alerting are made efficient by distributed blockchain-based IDPS. A peer-to-peer blockchain network is a foundation for this IDPS architecture, making monitoring expansive networks for malicious activity easier [11]. Since the data is stored and monitored in a distributed manner, malicious activities can be detected more quickly in this way compared to conventional methods. Additionally, the blockchain-based system enables quick network log data retrieval, which can be used for security alert notifications [12]. The distributed blockchain-based IDPS offers a novel method for enhancing security measures for huge networks.

Machine Learning-Based IDPS

As ML algorithms are fed datasets containing benign and malicious activities using algorithms like deep learning (DL) or support vector machine (SVM), the use of machine learning-based IDPS for anomaly detection greatly aids in its capacity as a form of intrusion detection and prevention system. These ML algorithms can be trained to more effectively identify malicious or malicious-looking activities, accurately detecting potential anomalies and ultimately giving the user higher levels of security [6].

Artificial Intelligence-Based IDPS

AI-based intrusion detection and prevention systems are increasingly viewed as a step toward increasing the system's accuracy and responsiveness. Artificial intelligence (AI) algorithms can examine network protocols and spot suspicious patterns in real-time, allowing for more accurate and rapid threat detection [13]. Thus, it has emerged as a dependable complement to established defenses, particularly in developing cyber threats. AI-driven IDPS solutions speed up response to cyberattacks, reducing the risk of data leakage and other security issues [14]. Additionally, the real-time analysis of traffic patterns facilitates the ability to identify the source of intrusions. More effective defenses against potential threats are produced by such precision [15]. IDPS deployment is made appealing by the increased accuracy and quick response of AI-based IDPS.

*Testing and Results*

Using real-world datasets, including the DARPA 99 and MIT-Lincoln Labs datasets, as well as our unique datasets, we tested our proposed methodology. Accuracy and false positive rate were the two metrics we used to assess the system. The system achieved 92.6% accuracy and 7.4% false positive rates. These findings show that the suggested methodology significantly lowers the false positive rate while increasing the accuracy of current blockchain-based IDPS.

Results

Based on a real-world dataset, the proposed system's accuracy was assessed. In Table, I, the evaluation's findings are displayed.

|  |  |
| --- | --- |
| Method | Accuracy |
| Proposed System | 92.6% |
| Existing System | 85.2% |

Table I: Evaluation findings

*Conclusion*

This paper proposes a novel methodology for improving accuracy in blockchain-based IDPS. The method, which has been presented, is based on combining various IDPS algorithms to detect intrusion attempts and utilizing a blockchain-integrated architecture to boost the system's scalability and accuracy. Multiple datasets were used to test the proposed methodology, and the results showed that our system significantly increases the accuracy of current blockchain-based IDPS while lowering the false positive rate. Our research findings offer new opportunities for developing highly accurate networks with a lower risk of false positives, which can be helpful to other researchers working on blockchain-based security solutions.

*Conflict of Interest Disclosure*

This research declares no conflict of interest.

*Acknowledgment*

Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University.

**References**

1. F. F. Alruwaili, “Intrusion Detection and Prevention in Industrial IoT: A Technological Survey,” IEEE Xplore, Oct. 01, 2021. <https://ieeexplore.ieee.org/abstract/document/9590961/> (accessed Jun. 08, 2023).
2. N. Mazhar, R. Salleh, M. Asif, and M. Zeeshan, “SDN based Intrusion Detection and Prevention Systems using Manufacturer Usage Description: A Survey,” International Journal of Advanced Computer Science and Applications, vol. 11, no. 12, 2020, doi: <https://doi.org/10.14569/ijacsa.2020.0111283>.
3. S. Latif, Z. Idrees, Z. e Huma, and J. Ahmad, “Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions,” Transactions on Emerging Telecommunications Technologies, Jul. 2021, doi: <https://doi.org/10.1002/ett.4337>.
4. H. Taherdoost, “Blockchain and Machine Learning: A Critical Review on Security,” Information, vol. 14, no. 5, p. 295, May 2023, doi: <https://doi.org/10.3390/info14050295>.
5. V. Wylde et al., “Cybersecurity, Data Privacy and Blockchain: A Review,” SN Computer Science, vol. 3, no. 2, Jan. 2022, doi: <https://doi.org/10.1007/s42979-022-01020-4>.
6. S. Zaman, Haseeb Tauqeer, W. Ahmad, A. Shah, and M. Ilyas, “Implementation of Intrusion Detection System in the Internet of Things: A Survey,” Nov. 2020, doi: <https://doi.org/10.1109/inmic50486.2020.9318047>.
7. M. Rabbani et al., “A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies,” Entropy, vol. 23, no. 5, p. 529, Apr. 2021, doi: <https://doi.org/10.3390/e23050529>.
8. Y. Al-Hadhrami and F. K. Hussain, “Real time dataset generation framework for intrusion detection systems in IoT,” Future Generation Computer Systems, vol. 108, pp. 414–423, Jul. 2020, doi: <https://doi.org/10.1016/j.future.2020.02.051>.
9. A. Khraisat and A. Alazab, “A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges,” Cybersecurity, vol. 4, no. 1, Mar. 2021, doi: <https://doi.org/10.1186/s42400-021-00077-7>.
10. J. Arshad, M. A. Azad, M. Mahmoud Abdellatif, M. H. Ur Rehman, and K. Salah, “COLIDE: a collaborative intrusion detection framework for Internet of Things,” IET Networks, vol. 8, no. 1, pp. 3–14, Jan. 2019, doi: <https://doi.org/10.1049/iet-net.2018.5036>.
11. S. S. Mathew, K. Hayawi, N. A. Dawit, I. Taleb, and Z. Trabelsi, “Integration of blockchain and collaborative intrusion detection for secure data transactions in industrial IoT: a survey,” Cluster Computing, vol. 25, no. 6, pp. 4129–4149, Jun. 2022, doi: <https://doi.org/10.1007/s10586-022-03645-9>.
12. E. S. Babu et al., “Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks,” Computers and Electrical Engineering, vol. 103, p. 108287, Oct. 2022, doi: <https://doi.org/10.1016/j.compeleceng.2022.108287>.
13. A. Bécue, I. Praça, and J. Gama, “Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities,” Artificial Intelligence Review, Feb. 2021, doi: <https://doi.org/10.1007/s10462-020-09942-2>.
14. H. Liu, C. Zhong, A. Alnusair, and S. R. Islam, “FAIXID: A Framework for Enhancing AI Explainability of Intrusion Detection Results Using Data Cleaning Techniques,” Journal of Network and Systems Management, vol. 29, no. 4, May 2021, doi: <https://doi.org/10.1007/s10922-021-09606-8>.
15. R. Kaur, D. Gabrijelčič, and T. Klobučar, “Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions,” Information Fusion, p. 101804, Apr. 2023, doi: <https://doi.org/10.1016/j.inffus.2023.101804>.