Journal of Current Research in Engineering and Science
JCRES
Bi-Annual Online Journal (ISSN: 2581 - 611X)

VOLUME:8, ISSUE:1, FEBRUARY 2025, PAPER NUMBER:50

Machine Learing - A Reinforcement algorithm to detect the malicious attack in Blockchain

P. Preethy Jemima
Department of Computing Technologies,
SRM Institute of Science and Technology,
Kattankulathur.
Preethy.jemima@gmail.com

C. Pretty Diana Cyril,
Department of Computing Technologies,
SRM Institute of Science and Technology,
Kattankulathur.
prettydianacyril@gmail.com

Abstract:

In the context of blockchain technology, a 51% attack occurs when one or more entities control more than 50% of the network's processing, mining, or hashing capacity. Because of this, they are able to manage the consensus mechanism of the network, giving them the ability to modify transactions, control their order, and maybe interfere with the blockchain's regular operation.They also suffer from double spending,transaction rejection , reverse a transaction as well as network disruption.These algorithms can immediately mitigate an attack by raising alarms or initiating automated responses based on continuous network activity monitoring. Based on input from the network environment, adaptive solutions for countering 51% attacks can be created using reinforcement learning algorithms. These algorithms can dynamically modify defence measures to preserve network security and adapt to changing attack techniques by continuously learning from and improving their decision-making processes. Blockchain protocols can benefit from the direct integration of machine learning algorithms to strengthen their resistance against 51% attacks. Consensus algorithms, for instance, can include machine learning-based methods to validate and verify blocks, guaranteeing that the blockchain contains only authentic transactions.

Keywords: *Consensus algorithm, Blockchain, reinforcement learning algorithms, double spending, reverse transaction , Machine Learning.*

I. INTRODUCTION

Blockchain is a distributed, decentralised ledger technology that maintains the integrity, transparency, and security of data shared by recording transactions series of blocks connected in chronological order that each include a list of transactions, establishing a continuous chain. A few of the most important aspects of blockchain:

Decentralisation: A copy of the complete blockchain is stored on each node of the peer-to-peer network of computers, or "nodes," on which blockchain functions. Because it is decentralised, there is no longer a need for a centralised authority or middleman, enabling members to interact directly and without trust.

Transparency: All network users can see every transaction that is registered on the blockchain. Because it is difficult to change or tamper with transaction records without the approval of the majority of the network, this transparency assures accountability and prevents fraud.

Immutability: A transaction cannot be

changed or removed after it is registered on the blockchain and approved by the network via a procedure known as consensus. The permanence and integrity of the data stored on the blockchain are guaranteed by its immutability.

Machine learning (ML) algorithms represent a powerful approach to overcoming these challenges, offering the ability to analyze large datasets of malicious data. By applying Machine learning approaches we can stop double spensing and reverse a transaction. Even network disruption can also be stopped. This analysis not only contributes to the theoretical understanding but also has practical implementation. In application to the historical logs of ethereum we can make use of the attributes to ensure the reliability of a transaction. Making use of the hash algorithm the key used is hard to be tampered.

II. RELATED WORKS

In the domain of blockchain , particularly for threat detection or malicious activity tracking, recent advancements have leveraged machine learning techniques to enhance the efficiency and integrity. This section reviews related works that have significantly contributed to the field by improving the reliability and various techniques and applications where we can make use of this blockchain technologies decentralized nature using machine learning approaches.

Consensus Mechanisms is exploring the security implications of different consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), and others. 51% Attacks is analyzing the security risks associated with a single entity controlling the majority of the network's mining power [1].

Integration with Blockchain is the monitoring system integrates with blockchain technology to enhance security and transparency. This could involve recording security-related events or data on the blockchain for immutable storage and auditability. Network Security Functions is detailing the specific security functions monitored by the system, such as intrusion detection, firewall performance, access control, and data encryption [2].

Mitigation Strategies such as implementing robust consensus mechanisms, conducting thorough code audits for smart contracts, and enhancing data encryption and privacy protocols.Cloud-Specific Considerations are given the deployment of the blockchain platform in cloud environments, the author may also address security considerations specific to cloud computing, such as securing cloud infrastructure, managing access controls, and ensuring compliance with relevant regulations [3].

An overview of the unique characteristics and challenges of vehicular networks, including high mobility, intermittent connectivity, and the need for secure and reliable communication.Assessment of the performance and effectiveness of the blockchain-based security mechanism through simulations, experiments, or real-world deployments. This could include metrics such as latency, throughput, security overhead, and resilience to attacks [4].

Data Encryption is ensuring data confidentiality through encryption techniques.Access Control is implementing access control policies using smart contracts to regulate data access and permissions.
Data Integrity Verification is utilizing blockchain's immutable ledger to verify the integrity of stored data and detect unauthorized modifications. Auditing and Compliance is using blockchain to maintain an audit trail of data access and modifications for compliance purposes [5].

Immutable Audit Trail is leveraging blockchain's immutable ledger to maintain an audit trail of authentication transactions, enhancing transparency and accountability. Lightweight Protocol Design is designing lightweight communication protocols suitable for resource-constrained IoT devices to minimize computational and energy overhead [6].

Malicious Attacks and Intrusion Prevention is likely elaborates on various types of malicious attacks and intrusions commonly targeting IoT networks, such as DDoS attacks, malware injection, and unauthorized access [7].

Smart Contracts for Governance is implementing smart contracts to define and enforce governance rules, access control policies, and transaction validation mechanisms within the IoV network.[8]

Smart Contracts for SLA Enforcement is implementing smart contracts to define and enforce service level agreements (SLAs) between service providers and consumers, ensuring that performance metrics meet predefined criteria.

Immutable Performance Records is leveraging blockchain's immutable ledger to store performance records, ensuring data integrity and facilitating auditability [9].

Incorporating Capsule Network techniques for efficient data representation and analysis, enabling the system to detect and respond to security threats effectively and Implementing a Situation Awareness framework to provide a comprehensive understanding of the security posture and identify emerging threats or vulnerabilities [10].

III. PROBLEM STATEMENT

By starting a transaction on the blockchain, transferring the tokens to a different address, and then starting a fork where the first transaction never happened, the attacker can spend the same cryptocurrency tokens twice. They can now use the same tokens in the authorised chain. An attacker has the ability to stop other miners from verifying transactions by seizing the majority of the mining power. They can accomplish this by blocking or rejecting transactions, which will essentially stop the network from processing new transactions. Because a 51% attack compromises the fundamental ideas of decentralisation and trustlessness, which form the foundation of blockchain technology, it presents a serious danger to the security and integrity of a blockchain network. It may cause monetary losses, interfere with network functioning.

IV. PROPOSED WORK

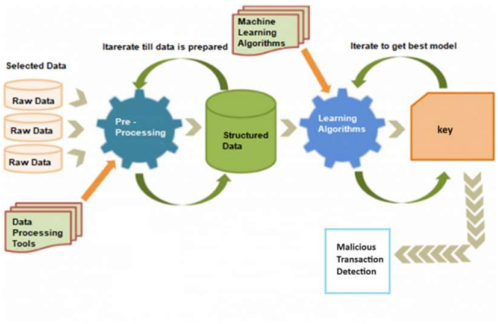

Fig:1 Architeccture Diagram

In the context of blockchain, reinforcement learning (RL) entails applying RL algorithms to enhance and optimise different parts of blockchain systems. While Proof of Work (PoW) and Proof of Stake (PoS) are the consensus processes that blockchain technology has historically relied on, RL can be used to improve the scalability, security, and efficiency of blockchain networks. Here are a few possible blockchain uses for RL:

Consensus Mechanism Optimisation: RL algorithms can be used to dynamically modify parameters like block size, block interval, and mining difficulty in order to optimise consensus mechanisms. This can support the preservation of security and decentralisation while enhancing the throughput and latency of blockchain networks.

Adaptive Network Routing: To enhance data transmission and lower latency in blockchain networks, RL algorithms can optimise network routing protocols. The best paths for blocks and transactions to propagate over the network can be dynamically chosen by RL agents using performance metrics and network topology as learning tools.

Security and Attack Detection: RL algorithms are useful in identifying and thwarting a range of security risks and assaults in blockchain networks, including double-spending, selfish mining, and 51% attacks. Through acquiring the ability to identify malevolent behaviour patterns and unusual conduct.

V. IMPLEMENTATION AND RESULTS

Training and validation are fundamental concepts in machine learning (ML) and are crucial stages in the development of ML models.

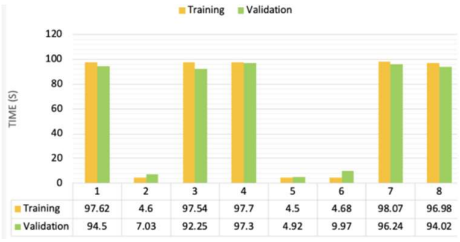

Fig:2 Training and validation

An ML algorithm is trained when labelled data is fed into it so that it can identify patterns and correlations in the data. Based on the input data and related labels, the algorithm modifies its internal parameters during training.During training, models are usually assessed for performance and generalizability using a different validation dataset. This lessens the chance of overfitting, in which the model recognises the malicious input clearly and retains the training data.

The process of evaluating a trained machine learning model's performance on data that it was not exposed to during training is known as validation. It assists in assessing the model's generalizability to fresh, untested data and detecting any problems.

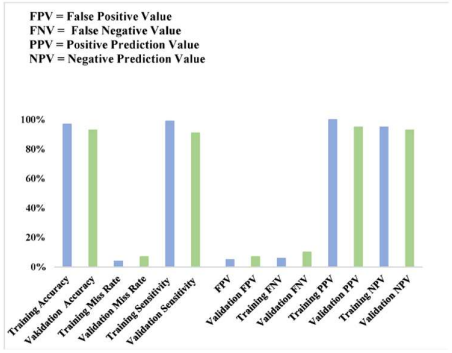

Fig : 3 Representation of FPV,FNV,PPV,NPV

The state of the blockchain network, including transaction history, network architecture, and performance indicators, can be represented by RL agents in a way that makes them amenable to learning. Features like transaction volume, transaction frequency, node connectivity, and transaction confirmation times might be included in this representation.

Reward Signal: Based on their observations and behaviour within the blockchain network, RL agents are rewarded with signals. The incentive signal in the context of identifying malicious data can be determined by the agent's accuracy in recognizing and flagging suspicious transactions or network activity. When an agent properly detects a fraudulent transaction, for instance, it gets rewarded positively; conversely, when it incorrectly labels legal transactions as malicious, it gets rewarded negatively.

VI. CONCLUSION

In conclusion, the system is built and works on the basis of training and validation only. The machine learning- reinforcement algorithm main works in the basis of rewards. Correct detection leads to the successful transaction with a positive rewards where as in false prediction goes with negative reward.Our system model after continuous training the model produces 95% of accuracy. As the the successful identification of threats are done which stops the attacker to take the control of the transaction by which we are able to put an end to double spending as well as reverse transaction.

REFERENCES

1. M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, M. H. S. Mohamad and A. H. Embong, "A Review on Blockchain Security Issues and Challenges," 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2021, pp. 227-232, doi: 10.1109/ICSGRC53186.2021.9515276.

2. J. J. Kim, P. Lingga, J. P. Jeong, Y. Choi and J. Park, "A Web-Based Monitoring System of Network Security Functions in Blockchain-Based Cloud Security Systems," 2022 International Conference on Information Networking (ICOIN), Jeju-si, Korea, Republic of, 2022, pp. 454-459, doi: 10.1109/ICOIN53446.2022.9687177.

3. P. Ruf, J. Stodt and C. Reich, "Security Threats of a Blockchain-Based Platform for Industry Ecosystems in the Cloud," 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 2021, pp. 192-199, doi: 10.1109/WorldS451998.2021.9514058.

4. G. Yan, "BlockChain Based Data Security Mechanism for Vehicular Networks," 2023 6th International Conference on Electronics Technology (ICET), Chengdu, China, 2023, pp. 658-663, doi: 10.1109/ICET58434.2023.10211276.

5. M. A. Z. Bin Idrus, F. D. A. Rahman, O. O. Khalifa and N. M. Yusoff, "Blockchain-based

Security for Cloud Data Storage," 2023 IEEE 9th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Kuala Lumpur, Malaysia, 2023, pp. 73-77, doi: 10.1109/ICSIMA59853.2023.10373457.
6. X. Yang et al., "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3321-3332, 1 March1, 2022, doi: 10.1109/JIOT.2021.3098007.
7. R. K. Sharma and R. S. Pippal, "Malicious Attack and Intrusion Prevention in IoT Network using Blockchain based Security Analysis," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 2020, pp. 380-385, doi: 10.1109/CICN49253.2020.9242610.
8. D. Das, S. Banerjee, W. Mansoor, U. Biswas, P. Chatterjee and U. Ghosh, "Design of a Secure Blockchain-Based Smart IoV Architecture," 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), DUBAI, United Arab Emirates, 2020, pp. 1-4, doi: 10.1109/ICSPIS51252.2020.9340142.
9. K. TaeYoung and K. Hyung-Jong, "Blockchain-based Service Performance Evaluation Method Using Native Cloud Environment," 2020 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, USA, 2020, pp. 52-52, doi: 10.1109/ICSSA51305.2020.00016.
10. L. Boheng, "Construction Strategy of Enterprise Security Management Blockchain based on Capsule Network and Situation Awareness1," 2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Penghu, Taiwan, 2021, pp. 1-2, doi: 10.1109/ICCE-TW52618.2021.9603157.
11. M. A. Ferrag and L. Shu, "The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial," in IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17236-17260, 15 Dec.15, 2021, doi: 10.1109/JIOT.2021.3078072.
12. S. Ismail and H. Reza, "Security Challenges of Blockchain-Based Supply Chain Systems," 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, NY, USA, 2022, pp. 1-6, doi: 10.1109/UEMCON54665.2022.9965682.
13. S. Matsuo, "How formal analysis and verification add security to blockchain-based systems," 2017 Formal Methods in Computer Aided Design (FMCAD), Vienna, Austria, 2017, pp. 1-4, doi: 10.23919/FMCAD.2017.8102228.
14. A. Mitra, B. Bera and A. K. Das, "Design and Testbed Experiments of Public Blockchain-Based Security Framework for IoT-Enabled Drone-Assisted Wildlife Monitoring," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 2021, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484468.
15. S. L. Ribeiro and I. A. de Paiva Barbosa, "Risk Analysis Methodology to Blockchain-based Solutions," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 2020, pp. 59-60, doi: 10.1109/BRAINS49436.2020.9223309.

About the Author :

P.Preethy Jemima is a Research Scholar in the Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, India. She received her B.E. in Computer Science and Engineering from National College of Engineering and M.E. in Computer Science and Engineering from SA engineering College. She has 4 years of teaching experience. Her research interests include Blockchain, Machine Learning, Image processing and Internet of Things.

C.Pretty Diana Cyril is working as an Assistant Professor in the Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur campus, Chennai, India. Her disciplines Software Engineering, Artificial Intelligence.