International Journal of Gender, Science and Technology
ISSN: 2040-0748
UGC Care Group I Journal.
Vol-14 Issue-01 Mar 2025

Collaborative Education for Blockchain Network Cyberattack Detection

[1]S SURYA KUMARI, [2]Dr POTNURI SURIBABU

[1]PG Scholar, Dept. of CSE, KMM Institute of Technology And Science, Tirupati, AP, India.

[2]Professor, Dept. of CSE, KMM Institute of Technology And Science, Tirupati,AP, India.

Abstract: The purpose of this paper is to examine infiltration assaults and then provide a new methodology for detecting cyberattacks at the network layer of blockchain networks, such as flooding of transactions and brute password attempts. In particular, we start by creating and setting up a blockchain network in our lab. This blockchain network will be used to provide actual traffic data (both normal and attack data) for our learning models and to conduct experiments in real time to assess how well our suggested intrusion detection system performs. As far as we are aware, this is the first dataset for blockchain network cyberattacks to be synthesised in a lab. Next, we provide a brand-new collaborative learning approach that enables effective implementation in the blockchain network for attack detection. The primary concept of the suggested learning model is to allow blockchain nodes to actively gather data, use the Deep Belief Network to learn from the data, and then communicate what they have learnt with other blockchain nodes in the network. In this manner, unlike traditional centralised learning techniques, we may not only benefit from the expertise of every node in the network but also avoid the requirement to collect all raw data for training at a single node. Such a framework can help prevent excessive network overhead/congestion and the danger of revealing the privacy of local data. Our suggested intrusion detection architecture can identify assaults with an accuracy of up to 98.6%, as demonstrated by both real-time trials and rigorous simulations.

INDEX TERMS: Blockchain, deep learning, collaborative learning, cyberattack detection, intrusion detection.

1. INTRODUCTION

Blockchain technology has emerged as a revolutionary approach to data management, offering decentralization, immutability, and enhanced security over traditional systems. However, with its increasing adoption in various sectors, blockchain networks have become prime targets for cyberattacks, particularly in cryptocurrency exchanges and critical applications like healthcare and supply chains. Conventional authentication methods, while effective for access control, fail to detect sophisticated attacks such as Flooding of Transactions (FoT) and Brute Password (BP) attacks. To address these threats, intrusion detection systems (IDS) are essential for identifying malicious activities post-authentication. Recent research has explored various ML-based IDS techniques to detect attacks in blockchain networks, demonstrating high accuracy in identifying anomalies. However, existing solutions often rely on

datasets not specifically designed for blockchain traffic, limiting their effectiveness in real-world scenarios.

While some studies have attempted to generate synthetic blockchain attack datasets using artificial intelligence and controlled experiments, they face limitations in accuracy and scalability. Most ML-based intrusion detection systems for blockchain rely on centralized learning models, which are unsuitable for decentralized networks due to privacy concerns and the impracticality of sharing raw traffic data among nodes. Centralized models can also cause network congestion and risk data integrity issues. The lack of a standardized, real blockchain dataset for training ML models remains a significant challenge, making it difficult to effectively detect diverse and evolving cyber threats in blockchain environments.

To overcome these challenges, this study introduces the Blockchain Network Attack Traffic (BNaT) dataset, generated from a real Ethereum-based blockchain network in a controlled laboratory environment. BNaT ensures clean and accurate data samples, incorporates various real-world blockchain attacks, and captures decentralized attack behaviors more effectively than previous artificial datasets. Additionally, the study proposes a decentralized collaborative ML framework for intrusion detection, allowing nodes to detect attacks without sharing sensitive raw data. This approach enhances privacy, maintains network efficiency, and improves the adaptability of IDS solutions to evolving cyber threats in blockchain networks.

2. LITERATURE SURVEY

2.1 Applications of Blockchains in the Internet of Things: A Comprehensive Survey:

https://ieeexplore.ieee.org/abstract/document/8580364

ABSTRACT: With the advent of the groundbreaking cryptocurrency platform Bitcoin, blockchain technology has completely transformed the digital currency market. An abstract definition of a blockchain is a distributed ledger that can preserve an unchangeable record of all network transactions. In recent years, this technology has garnered a lot of scholarly attention in fields other than finance, such the Internet of Things (IoT). In this regard, the blockchain is viewed as the final component needed to create an IoT ecosystem that is genuinely decentralised, trustless, and safe. Our goal in conducting this survey is to provide a clear and thorough overview of the state-of-the-art initiatives currently underway in this regard. We begin by discussing the basic concepts of blockchain technology and how decentralisation, security, and auditability are achieved in blockchain-based systems. After discussing the difficulties presented by the existing centralised IoT models, we go on to discuss recent developments in business and research that address these issues and successfully employ blockchain technology to offer a decentralised, secure IoT medium.

2.2 A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges:

https://ieeexplore.ieee.org/document/8642861

ABSTRACT: The world's population has been rapidly urbanising in recent years, leading to a

number of economic, social, and environmental issues that have a substantial impact on people's quality of life and living circumstances. These urban issues can be resolved with the help of the "smart city" idea. The goals of smart cities are to maximise the use of public resources, offer inhabitants first-rate services, and enhance the standard of living for all. The deployment of smart cities heavily relies on information and communication technologies. Blockchain is a new technology with many positive aspects, including transparency, democracy, automation, decentralisation, security, transparency, and pseudonymity. These blockchain characteristics aid in advancing the growth of smart cities and enhancing their offerings. We present a thorough review of the literature on blockchain technology's application to smart cities in this article. First, background information and relevant works are presented. The use of blockchain technology in smart cities is then examined from the viewpoints of supply chain management, smart grid, smart transportation, smart citizens, and smart healthcare, among others. Lastly, a few issues and more general viewpoints are covered.

2.3 A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV

https://www.researchgate.net/publication/340999302_A_Survey_of_Network_Virtualization_Techniques_for_Internet_of_Things_Using_SDN_and_NFV

ABSTRACT: Network softwarization and the Internet of Things (IoT) are quickly emerging as key technologies for information systems and network administration in the context of the next-generation Internet. Smart cities, urban computing, omnipresent healthcare, and tactile Internet are just a few examples of how the Internet of Things is being deployed and used. Because of this, heterogeneous network systems' physical infrastructure has grown more complex, necessitating effective and flexible management, configuration, and flow scheduling solutions. Recent years have seen a great deal of study on network softwarization for the Internet of Things in the form of Software Defined Networks and Network Function Virtualisation. We provide a thorough and methodical analysis of virtualisation strategies specifically created for Internet of Things networks in this post. The literature has been divided into three categories: software-de-ned IoT networks, function virtualisation for IoT networks, and software-de-ned networks built for IoT. These groups are further subdivided into works that offer management, security, and architectural solutions. In addition, the essay identifies a number of ongoing problems and short- and long-term research difficulties pertaining to the implementation of software-defined IoT.

2.4 Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities

https://ieeexplore.ieee.org/document/8746079

ABSTRACT: In recent years, blockchain technology's explosive growth and wide range of new applications have drawn a lot of interest. The foundation of a blockchain network is the distributed consensus process. It is essential to maintaining the security, integrity, and functionality of the network. The proof-of-work consensus techniques, which rely

on heavy mining operations to establish an agreement, have been implemented by the majority of contemporary blockchain networks. Nevertheless, this technique has a number of drawbacks, including inefficiency in terms of energy, latency, and susceptibility to security risks. A novel consensus technique called proof of stake was created lately to address these issues. It allows for consensus to be reached by demonstrating stake ownership. It is anticipated that this method will develop into a state-of-the-art technology for next blockchain networks. The goal of this paper is to examine proof-of-stake mechanisms, from basic concepts to sophisticated protocols based on proof-of-stake, as well as performance analysis, including energy consumption, delay, and security, and their potential uses, especially in the Internet of Vehicles. Additionally, the development of stake pools and their impact on the distribution of network stakes are examined and modelled. The findings indicate that the decentralisation of the network is significantly influenced by the ratio of the block reward to the total network stake. There is also discussion of technical difficulties and possible fixes.

2.5 Anomaly Detection in Blockchain Networks: A Comprehensive Survey

https://ieeexplore.ieee.org/abstract/document/9887797

ABSTRACT: Because blockchain technology can be connected with so many commonplace uses of contemporary information and communication technologies (ICT), it has garnered significant interest from both industry and academics over the past 10 years. Blockchain's peer-to-peer (P2P) design improves these applications by offering robust security and trust-oriented assurances including decentralisation, immutability, and verifiability. Notwithstanding the amazing benefits that blockchain technology offers these ICT applications, recent studies have shown that the robust assurances are insufficient, and blockchain networks may nonetheless be vulnerable to a number of security, privacy, and dependability problems. Finding the unusual conduct within the actionable time range is crucial to resolving these problems. We offer a thorough analysis of the incorporation of anomaly detection algorithms into blockchain technology in this paper. To do this, we first go over how anomaly detection may help make blockchain-based apps more secure. Next, we present several essential assessment criteria and prerequisites that might be crucial in the process of creating blockchain anomaly detection models. We then provide an in-depth analysis of many anomaly detection techniques from the viewpoint of every blockchain layer. We wrap up the paper by outlining several significant issues and talking about how they may be used as future lines of inquiry for fresh investigators in the area.

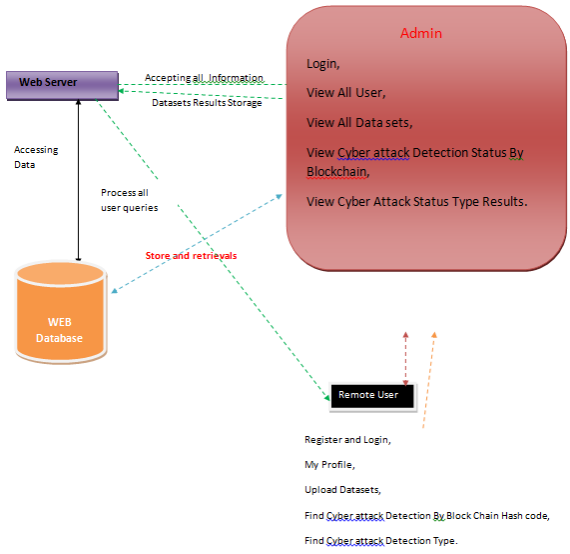
3. METHODOLOGY

a) Proposed Work:

The goal of our suggested model is to use the information that each node in the network has acquired in a decentralised way without disclosing their raw data (i.e., labelled training datasets). In order to accomplish this, we first create a framework for the decentralised blockchain network where each learning node—that is, every node in the network—deploys a deep learning model (more information will be provided in the next section) to learn from the data it has gathered. After that, it shares its trained

model with a Centralised Server (CS). In the blockchain network, the CS might be any complete node or a bootnode. After then, the CS will combine all of the learnt models and return the combined model—also known as the global model—to the learning nodes that took part. The learning nodes can eventually achieve convergence (to the global training model) by iteratively updating their deep learning models. By doing this, we can reduce the danger of revealing local information about learning nodes throughout the network and increase the precision of identifying cyberattacks in blockchain networks. Our suggested approach can identify cyberattacks in the network under consideration with an accuracy of up to 98.6%. Furthermore, by extracting information from shared trained models, nodes in our suggested learning model can still gain valuable information from other nodes in the network without having to share their raw data.

b) System Architecture:



The proposed system architecture consists of a decentralized intrusion detection framework designed specifically for blockchain networks. It incorporates multiple nodes within a blockchain environment, each equipped with a local machine learning (ML) model for detecting malicious activities. Instead of relying on a centralized server, each node independently analyzes network traffic and applies anomaly detection techniques to identify potential threats such as Flooding of Transactions (FoT) and Brute Password (BP) attacks. This decentralized approach ensures that data remains within each node, preserving privacy and preventing unnecessary network congestion caused by centralized data sharing.

A key component of the architecture is the Blockchain Network Attack Traffic (BNaT) dataset, which serves as the foundation for training ML models. BNaT is generated from a real Ethereum-based blockchain environment, ensuring accurate representation of blockchain-specific attack patterns. Each node in the system leverages federated learning techniques to collaboratively enhance the accuracy of intrusion detection models. Instead of sharing raw data, nodes exchange encrypted model updates, allowing them to learn from distributed attack patterns while maintaining security and efficiency. This approach overcomes the limitations of traditional centralized ML models, which require raw data sharing and pose risks to data integrity.

To further improve detection accuracy, the system employs adaptive model updates and continuous learning mechanisms. As new threats emerge, nodes periodically update their local ML models based on recent attack patterns, ensuring that the intrusion detection system remains effective against evolving cyber threats. Additionally, the system integrates smart contract-based automation for real-time threat

response, enabling immediate countermeasures such as transaction blocking or alert generation. By combining decentralized ML-based intrusion detection, blockchain attack datasets, and automated response mechanisms, this architecture enhances the security, scalability, and efficiency of blockchain networks against sophisticated cyberattacks.

c) Modules:

Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View All User, View All Data sets, View Cyber attack Detection Status By Block chain, View Cyber Attack Status Type Results.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Register and Login, My Profile, Upload Datasets, Find Cyber attack Detection By Block Chain Hash code, Find Cyber attack Detection Type.

4. EXPERIMENTAL RESULTS

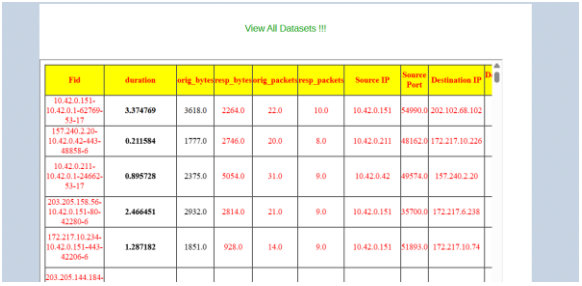


Fig 1:View Datasets

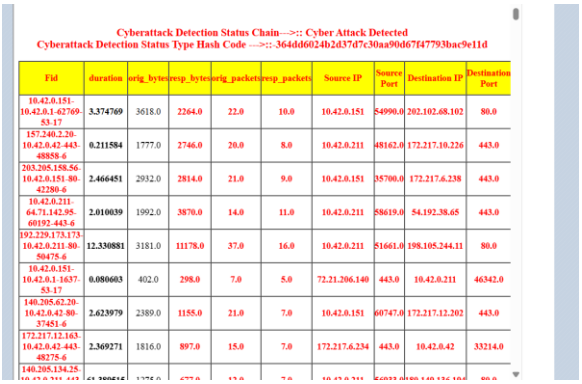


Fig 2: Cyberattack Detection Status Chain--->:: Cyber Attack Detected

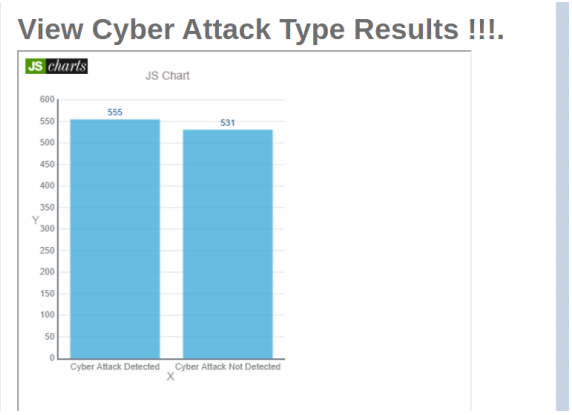


Fig 3: View Cyber Attack Type Results

5. CONCLUSION

In this paper, we have put forward a new collaborative learning architecture for a blockchain network cyberattack detection system. First, a private blockchain network has been put into place at our lab. In order to (1) create data (both normal and attack data) for the proposed learning models and (2) evaluate the effectiveness of our suggested learning framework in real-time trials, this blockchain network is utilised. Following that, we have put up a very successful learning model that enables its successful implementation on the blockchain network. By gathering data, learning from their data, and then sharing information to enhance attack detection capabilities, this learning approach enables nodes in the blockchain to actively participate in the detection process. By doing this, we can safeguard the blockchain network at its very edge while simultaneously avoiding the issues associated with traditional centralised learning, like as congestion and single points of failure. The effectiveness of our suggested architecture has since been amply demonstrated by simulation and real-time experimental data. We intend to keep expanding this dataset in the future to include more new attack types and provide stronger defences for blockchain networks.

6. FUTURE SCOPE

The future scope of this decentralized intrusion detection system for blockchain networks includes enhancements in model adaptability, scalability, and real-time threat mitigation. As blockchain technology evolves, integrating more advanced deep learning models and reinforcement learning techniques can significantly improve anomaly detection accuracy. These models can dynamically adapt to emerging attack patterns, reducing false positives and enhancing the overall security of blockchain transactions. Additionally, incorporating edge computing can further optimize processing efficiency, allowing intrusion detection to operate seamlessly on resource-constrained blockchain nodes.

Another promising direction is the expansion of the Blockchain Network Attack Traffic (BNaT) dataset by including a wider range of blockchain attack scenarios across different consensus mechanisms, such as Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS). This will enable the intrusion detection system to be more robust and applicable to diverse blockchain platforms. Furthermore, leveraging secure multi-party computation (SMPC) and homomorphic encryption techniques can enhance data privacy in federated learning, ensuring that model updates remain secure while improving detection efficiency.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H.Rehmani, “Applications of blockchains in the Internet of Things: Acomprehensive survey,” IEEE Communications Surveys & Tutorials,vol. 21, no. 2, pp. 1676–1717, Dec. 2018.

[3] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A surveyof blockchain technology applied to smart cities: Research issues andchallenges,” IEEE Communications Surveys & Tutorials, vol. 21, no. 3,pp. 2794–2830, Feb. 2019.
[4] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty,“Interoperability and synchronization management of blockchain-baseddecentralized e-health systems,” IEEE

Transactions on EngineeringManagement, vol. 67, no. 4, pp. 1363–1376, June 2020.

[5] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model,techniques, and applications," IEEE Transactions on Systems, Man, andCybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, July 2018.

[6] "The 10 Biggest Crypto Exchange Hacks InHistory," Accessed: Feb. 14, 2022. [Online].Available: https://crystalblockchain.com/articles/the-10-biggest-cryptoexchange-hacks-in-history

[7] "North Korean Hackers Have Prolific Year as TheirUnlaundered Cryptocurrency Holdings Reach All-time High,"Accessed: Feb. 14, 2022. [Online]. Available: https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-yearas-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high

[8] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen,and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for futureblockchain networks: fundamentals, applications and opportunities,"IEEE Access, vol. 7, pp. 85 727–85 745, Jun. 2019.

[9] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchainbasedsoybean traceability in agricultural supply chain," IEEE Access,vol. 7, pp. 73 295–73 305, May 2019.

[10] S. Bu, F. R. Yu, X. P. Liu, P. Mason, and H. Tang, "Distributed combinedauthentication and intrusion detection with data fusion in high-securitymobile ad hoc networks," IEEE transactions on vehicular technology,vol. 60, no. 3, pp. 1025–1036, Dec. 2010.

[11] X. Wang, X. Zha, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, andK. Zheng, "Attack and defence of ethereum remote apis," in 2018 IEEEGlobecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates,Dec. 2018, pp. 1–6.

[12] J. Ot´avio Chervinski, D. Kreutz, and J. Yu, "Analysis of transactionflooding attacks against Monero," in IEEE International Conference onBlockchain and Cryptocurrency (ICBC), Sydney, Australia, May 2021,pp. 1–8.

[13] J. Choi, B. Ahn, G. Bere, S. Ahmad, H. A. Mantooth, and T. Kim,"Blockchain-based man-in-the-middle (mitm) attack detection for photovoltaicsystems," in IEEE Design Methodologies Conference (DMC),July 2021, pp. 1–6.

[14] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki,"Network intrusion detection for IoT security based on learning techniques,"IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp.2671–2701, Jan. 2019.