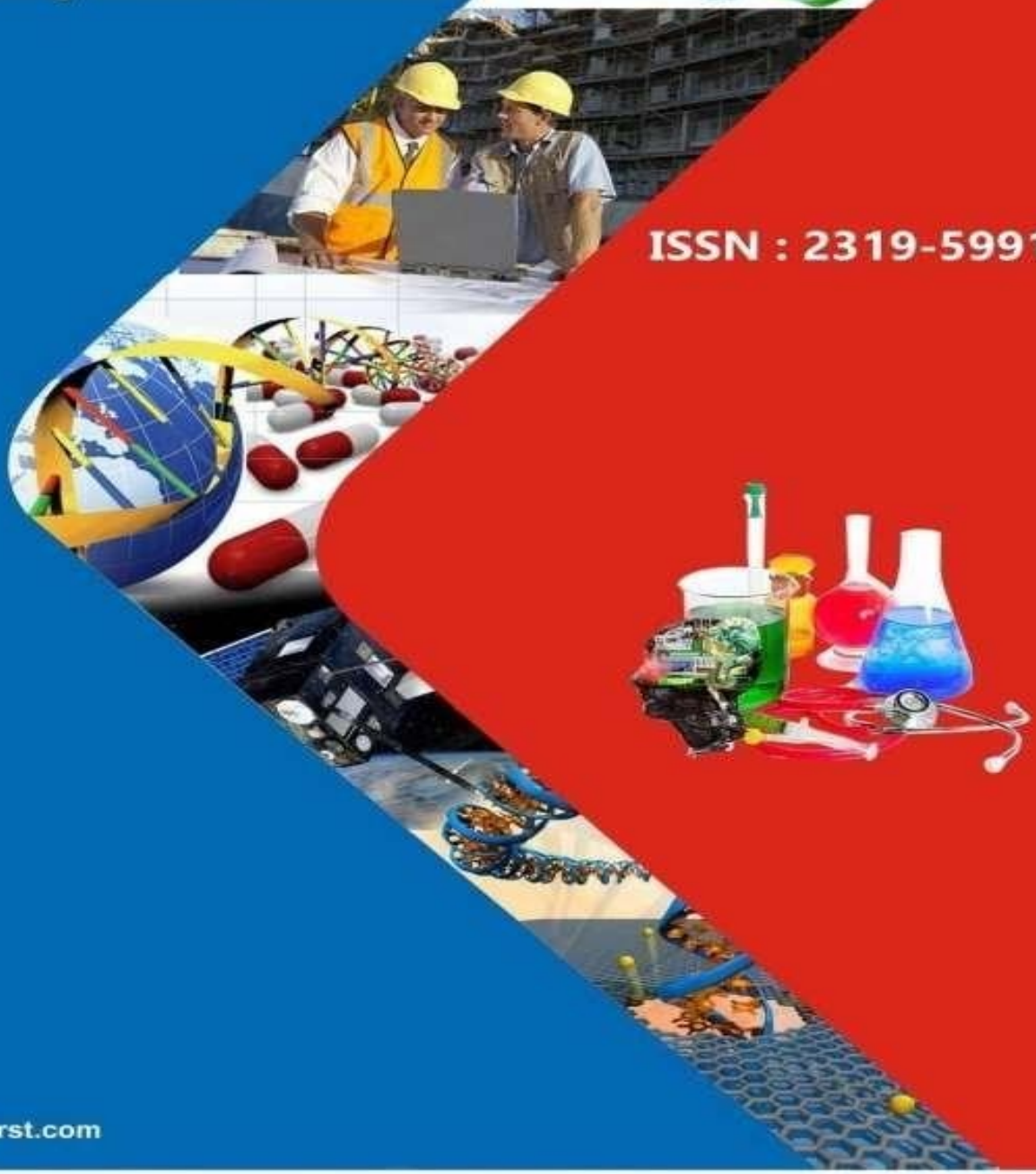
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653

Vol. 21, Issue 2, 2025

A COLLABORATIVE LEARNING FRAMEWORK FOR CYBERATTACK MITIGATION IN BLOCKCHAIN ENVIRONMENTS

[1]*Harijana Mahesh Kumar*, *MCA Student, Department of MCA*

[2] *Dr. B Mahesh, Ph.D, Associate Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

,

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 may 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 shown by both rigorous simulations and real-time trials.

I. INTRODUCTION

Emerging as a cutting-edge solution for data administration and storage, BLOCKCHAIN [1]–[3] offers several benefits over traditional data management methods. Specifically, block chain technology enables data to be kept in a distributed fashion across several nodes, in contrast to conventional centralised data management techniques. By doing this, bottlenecks and single points of failure may be avoided and data can be retrieved and processed concurrently at many nodes. The ability to store data in blocks—which is one of the most crucial aspects of block chain technology—means that once a block of data has been validated and added to the chain, it cannot be changed or removed. The exceptional qualities of blockchain, such as decentralisation, immutability, auditability, and fault tolerance, may therefore be used to safeguard the integrity of the data [2]. As a consequence, blockchain technology is being used in more and more areas of our life, such as IoT systems, healthcare, banking, and logistics [2]–[5].

Block chain-based systems have been the focus of several new-generation cyberattacks due to its quick success with a variety of applications in various fields, particularly money transfer and cryptocurrency. For instance, Singapore-based cryptocurrency exchange Ku Coin said in September 2020 that its system had been breached and that more than $281 million worth of coins and tokens had been taken [6]. One of the largest cryptocurrency exchanges in the world, Binance, was said to have had a significant security breach in May 2019. Customers lost almost $40 million as a result of the hackers' breach of the exchange's security infrastructure, which allowed them to remove over 7,000 bit coins from digital wallets [6]. Most recently, in January 2022, Chainalysis revealed that in 2021, North Korean hackers stole

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

around $400 million from digital assets via seven assaults on cryptocurrency platforms [7]. A variety of block chain applications in vital sectors including healthcare [8] and food supply chains [9] may soon be vulnerable to attackers, despite the fact that the majority of current assaults target virtual money exchange systems. In addition to causing enormous damages to our assets, these assaults have the potential to inflict other major problems pertaining to human health and life. As a result, it is more important than ever to find ways to identify and stop attacks in blockchain networks.

Authentication techniques, such as biometric technology and two-factor authentication, are used in network security to confirm and identify authorised users. We may make sure that only people or organisations with permission can access their systems or resources by putting authentication procedures in place. It is important to remember that, in spite of their advantages, authentication techniques are ineffective at stopping assaults on block chain networks. For instance, two of the most frequent attacks in block chain networks, Flooding of Transactions (FoT) and Brute Password (BP), are neither detectable or preventable by authentication techniques. In this situation, even after a user has been verified, intrusion detection systems may be used to spot unusual activity, such as the execution of malicious scripts or unauthorised instructions. We may strengthen the system's defences against cyberattacks by combining authentication techniques with intrusion detection systems [10]. To identify BP, FoT, or Man in the Middle (Mit M) attacks on blockchain networks, several investigations have been carried out [11]–[13]. In [11], the authors used a variety of devices (such as a Mac Book Pro, Mac Book Air, mobile phone, and Raspberry Pi) to conduct BP assaults in their test bed. They were then able to identify BP assaults by looking for unusually high CPU and memory use. The Monero blockchain network ledger was examined by the writers in [12] over a one-month period. In order to demonstrate how attackers make money via a FoT attack, they examined network bandwidth, block size, percentage of empty blocks, etc. For photovoltaic (PV) systems, the authors in [13] suggested a block chain-based technique for detecting MitM assaults. To store control instructions both before and after transmission, they used a smart contract. In order to identify MitM attacks, they compared these control command values. These techniques, however, exclusively target a certain kind of assault or are applied after harm has already been done. When compared to other traditional detection techniques like signature-based and abnormally-based, machine learning (ML) offers three key advantages for intrusion detection problems. ML has been regarded as the most effective way to identify cyberattacks in intrusion detection systems with high accuracies [14]–[16]. First off, machine learning (ML) solutions enable the simultaneous and highly accurate detection of several attack kinds, in contrast to traditional intrusion detection systems that are often built to identify a single attack type (such as a virus, trojan, spam, or botnet). Deep Learning (DL), for instance, can identify cyberattacks with an accuracy of up to 97.5% in industrial automation and control systems, including denial of service, reconnaissance, naïve malicious response injection, and complicated malicious response injection [17]. Second, machine learning (ML) makes it possible to identify attacks that have never been identified and reported before, while conventional solutions are often designed to identify known assaults. For instance, the authors demonstrated in [18] that their DL model is capable of detecting assaults like the Mirai DDoS attack and BASHLITE botnets, despite the fact that this model has never been taught to recognise or understand such operations. Finally, ML algorithms—DL in particular—can be implemented efficiently, rapidly, and adaptably. For instance, once trained, a deep neural network may be used simultaneously with various intrusion detection systems to swiftly and accurately identify cyberattacks. Furthermore, we

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

can readily upgrade new versions of deep neural networks using transfer learning methods when information about novel attack types becomes available [19].

Because of this, machine learning has been regarded as a very successful way to identify cyberattacks on blockchain networks [20]. In [21], for example, the authors suggested using Random Forest and XG Boost to identify assaults in an Internet of Things system that is based on the blockchain. The outcomes shown that with an accuracy of up to 99%, this system can distinguish between various assault kinds and typical behaviours. But they only used the BoT-IoT dataset, which isn't actual block chain traffic, to test their findings. Similarly, before the data is saved in the blockchain network, the authors of [22] suggested an ML-based technique called bidirectional long short-term memory (BiL STM) to identify assaults in an IoT network. They were only tested on standard network datasets like UNSW-NB15 and BoT-IoT datasets, despite the fact that the findings also shown that they can identify other attack types with an accuracy of up to 99%. Since these statistics were gathered on traditional computer networks, they are unable to accurately represent block chain network activity. Specifically, these datasets only include generic computer network attacks, not block chain-specific ones, such as altering block chain transactions, using the wrong consensus algorithm, or breaking the chain of blocks.

Two major issues that still need to be resolved for ML-based intrusion detection systems in block chain networks are evident from all of the aforementioned efforts as well as others in the literature. The first difficulty is specifically the scarcity of lab-generated synthetic data for ML model training. The majority of recent studies, such as [21] and [22], employed standard cyber security datasets for training, such as UNSW-NB15 and BoT-IoT. Nevertheless, these datasets are inappropriate for use in intrusion detection systems in block chain networks since they were not created for these networks. Other efforts, such as [23]–[25], attempted to construct their own datasets for block chain networks, for example, by producing fake attack samples using CGAN [24], constructing simulation experiments to identify the LFA [25], and acquiring the normal samples from the Bit coin network [23]. These approaches, however, have a number of problems. First off, all of the data that was gathered was categorised and labelled as regular data, even though typical samples of transactions from the Bitcoin network can include assaults from the public blockchain network. Second, in order to prevent them from extending to other assaults, the simulation experiment in [25] was designed to create trace route data only for the LFA. Additionally, it is challenging to assess whether or not the simulated attack samples in [24] can accurately mimic an actual assault on a blockchain network. Another issue is that all of the existing machine learning (ML)-based intrusion detection systems for blockchain networks rely on centralised learning models, meaning that all data is gathered at a single node for both detection and training. However, since blockchains are decentralised networks, this approach cannot be implemented there. Nodes in blockchain networks, in particular, could have different data to train, and they might not wish to share their raw data with a centralised node (or other nodes) for training procedures because of privacy issues. Note that the raw data refers to a local network's network traffic data. This data, which will be used for the learning process, may be divided into two categories: regular data and attack data. It often includes private data that the node does not wish to share with other nodes on the network, such as use ports, cryptographic keys, or local network bandwidth. Furthermore, transmitting a lot of data to the network might jeopardise the data integrity of block chain networks in addition to causing excessive network traffic.

In order to overcome the aforementioned difficulties, this paper first presents a new intrusion detection dataset called BNaT, or

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

Blockchain Network Attack Traffic, which was generated from an actual blockchain network in our lab. Next, it suggests a decentralised collaborative machine learning framework that is capable of detecting intrusions in the blockchain network. In particular, we use Ethereum, an open-source blockchain platform, to build up a blockchain network in our lab before conducting extensive experiments to produce blockchain data (both malicious and legitimate traffic data) in order to construct BNaT. The creation of the BNaT dataset has four primary goals. In order to get "clean" data samples—that is, data that is not tampered with, inaccurate, or irrelevant—we first gather the BNaT in a lab setting. This is particularly crucial for training machine learning models. Second, it is simple to expand the BNaT to include additional types of blockchain assaults, such as double spending or 51% attacks. Thirdly, we conduct tests using actual assaults in the blockchain network under consideration. As a result, the BNaT can more accurately represent the network's actual attack behaviour than simulations or fictional attack data produced by GAN in the literature, such as [24]. Fourth, we gather information from many blockchain nodes to get a comprehensive picture of the impact of decentralised assaults. Then, to improve its deployment in blockchain networks for threat detection, we create a highly efficient collaborative learning approach. Specifically, in our suggested learning model, blockchain network operating nodes (like full nodes) may be employed as learning nodes to gather data (such categorising data and watching incoming traffic). 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., training datasets with labels). Before sharing the trained model with a Centralised Server (CS), which can be a boot node or any full node in the blockchain network, we first design a framework for the decentralised blockchain network in which each participating learning node (i.e., full node in the blockchain network) deploys a deep learning model (more information will be provided in the next section) to learn from its collected data. After then, the CS will combine all of the learnt models and provide the combined model—also known as the global model—to the learning nodes that took part. The learning nodes may 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, under our suggested learning approach, nodes may still gain valuable information from other nodes in the network by extracting information from shared trained models, even if they are not required to share their raw data. The following is a summary of this paper's primary contributions.

• In order to test our suggested learning model in real-time and to collect genuine blockchain datasets, we set up experiments in our lab to construct a private blockchain network. We anticipate that our suggested BNaT dataset may support the development of ML-based intrusion detection systems in blockchain networks in the near future since, to the best of our knowledge, it is the first dataset acquired from a laboratory for researching cyberattacks in blockchain networks. Link 1 provides further information about the dataset.

• To gather information in the blockchain network, we develop an efficient technology called Blockchain Intrusion Detection (BC-ID). This program can filter attack samples in network traffic, precisely label them in real-time, and extract characteristics from the gathered network traffic data.

• We provide a collaborative decentralised learning methodology that can be successfully used in decentralised blockchain networks and

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

increase the precision of attack detection. Without having to disclose their raw data, this methodology allows all nodes in the blockchain network to efficiently communicate their trained models to increase the effectiveness of cyberattack detection.

• To assess our suggested framework, we conduct both in-depth simulations and live experiments. Our suggested framework outperforms existing basic machine learning techniques, as shown by both simulation and experimental findings. Additionally, our findings provide some crucial information for developing and putting into practice learning models in blockchain networks, such as real-time monitoring and threat detection.

This is how the remainder of the paper is structured. Basic background information, our blockchain network architecture, and the collaborative learning mechanism are all provided in Section II. Our suggested collaborative learning strategy for identifying cyberattacks in the blockchain network is presented in Section III. Section IV describes the experiment setup, dataset collection, and evaluation procedure; Section V goes into more depth on the experimental findings and performance assessments; and Section VI concludes the study.

1.1. Purpose Of The Project

With a focus on risks like transaction flooding and brute-force password attempts, this project intends to explore network-layer intrusion assaults and provide a novel cyberattack detection system for blockchain settings.

A specialised blockchain network is created and implemented in a controlled lab environment to assist this endeavour. The two primary functions of this environment are (1) to provide real-time experimental validation of the suggested detection framework and (2) to produce genuine traffic data, including both malicious and benign activity, for machine learning model training. Notably, this dataset is among the first resources for cyberattacks in a blockchain setting to be synthesised in a lab.

The project's main contribution is a brand-new collaborative learning paradigm designed for decentralised deployment. According to this paradigm, blockchain nodes gather data on their own, use Deep Belief Networks (DBNs) to learn from it, and then share the information they have extracted—rather than the raw data—with other nodes. By using dispersed intelligence across the network, this method not only improves detection capabilities but also decentralises learning, protecting data privacy and lowering network congestion.

The suggested architecture may reach detection accuracies of up to 98.6% in both rigorous simulations and real-time testing, demonstrating its effectiveness and practicality in protecting blockchain systems against changing cyberthreats.

1.2. EXISTING SYSTEM

To the best of our knowledge, only a small number of research take into account utilising actual blockchain traffic, such as attempts to produce fictional data or data that mimics an attack on blockchain networks in order to train machine learning models [23]–[25]. The authors specifically suggested a way to get blockchain traffic statistics in [23]. They started by taking traffic samples from a Bitcoin node that was open to the public and used them as standard network data. The authors then conducted DoS and Eclipse attacks on a target device (which was designed to function as a node in the Bitcoin network) in order to get the malicious traffic data. An autoencoder deep learning model was then trained using the gathered data. Up to 99% attack detection accuracy was shown by this method. The authors of [24] employed both a private and a public dataset from their test environment. They then suggested learning the characteristics of normal samples in the datasets using a Long Short-Term Memory Network (LSTM). They then created the synthetic Low-rate Distributed DoS (LDDoS) attack samples for their blockchain dataset using a Condition Generative Adversarial

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

Networks (CGAN) model. The findings showed a 93% classification accuracy.

Furthermore, in [25], the authors conducted a Link Flood assault (LFA) DDoS assault on a simulated Ethereum network and gathered the network's traceroute data under both attack and normal conditions. The authors then analysed the traceroute information using a Recurrent Neural Network (RNN) to find the network assaults. The findings shown that an assault detection rate of over 99% is possible.

The authors of [26] created a blockchain-based architecture that can identify a single assault, known as replay attacks, on a power system. Additionally, in [27], the authors suggested detecting cyberattacks for multimicrogrid systems by using blockchain technology and Support Vector Machines (SVM). Therefore, for blockchain-based systems, we create a decentralised learning model that can identify several attack types, such as Denial of Service (DoS), BP, and FoT.

Disadvantages

Two primary issues that still need to be resolved for ML-based intrusion detection systems in blockchain networks are evident from all of the aforementioned efforts as well as others in the literature. The first difficulty is specifically the scarcity of lab-generated synthetic data for ML model training. Conventional cybersecurity datasets, such as UNSW-NB15 and BoT-IoT, were utilised as training data in the majority of recent research, such as [21] and [22]. These datasets, however, are inappropriate for use in intrusion detection systems in blockchain networks since they were not created for blockchain networks. Other efforts, such as [23]–[25], attempted to construct their own datasets for blockchain networks, for example, by producing fake attack samples using CGAN [24], generating normal samples from the Bitcoin network [23], and developing simulation experiments to identify the LFA [25]. But these approaches have a number of problems.

1.3. PROPOSED SYSTEM

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 provide the combined model—also known as the global model—to the learning nodes that took part. The learning nodes may 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, our suggested learning approach allows nodes to learn from other nodes in the network by extracting information from shared trained models, even if they are not required to share their raw data.

Advantages

• In order to test our suggested learning model in real-time and to collect genuine blockchain datasets, we set up experiments in our lab to construct a private blockchain network. We anticipate that our suggested BNaT dataset may support the development of ML-based intrusion detection systems in blockchain networks in the near future since, to the best of our knowledge, it is the first dataset acquired from a laboratory for researching cyberattacks in blockchain networks. The link provides more information about the dataset.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

• To gather information in the blockchain network, we develop an efficient technology called Blockchain Intrusion Detection (BC-ID). In addition to filtering attack samples in network traffic and accurately labelling them in real-time, this program can extract characteristics from the gathered network traffic data.
• In order to increase attack detection accuracy and successfully implement it in decentralised blockchain networks, we suggest a collaborative decentralised learning paradigm. Without having to disclose their raw data, this methodology allows fullnodes in the blockchain network to efficiently communicate their trained models to increase the effectiveness of cyberattack detection.
• To assess our suggested framework, we conduct both in-depth simulations and live experiments. Our suggested framework outperforms existing basic machine learning techniques, as shown by both simulation and experimental findings. Additionally, our findings provide some crucial details for developing and putting into practice learning models in blockchain networks, such as real-time monitoring and threat detection.

II. REQUIREMENT AND ANALYSIS

2.1. LITERATURE SURVEY

2.1.1. Overview

"A Peer-to-Peer Electronic Cash System: Bitcoin,"
Nakamoto, S.
Online payments might be transmitted straight between parties without going thru a financial institution if electronic currency were just peer-to-peer. Part of the answer is offered by digital signatures, but the primary advantages are lost if a reliable third party is still needed to stop double-spending. We suggest using a peer-to-peer network to address the double-spending issue. In order to create a record that cannot be altered without repeating the proof-of-work, the network timestamps transactions by hashing them into a continuous chain of hash-based proof-of-work. The longest chain is evidence of both the sequence of events seen and the fact that it originated from the greatest CPU power pool. Nodes that are not working together to attack the network will continue to control the bulk of CPU power, generating the longest chain and outpacing attackers. The network itself needs very little organisation. Nodes are free to join and exit the network at any time, and the longest proof-of-work chain is accepted as evidence of what transpired during their absence. Messages are broadcast using best effort.
"A thorough survey of blockchain applications in the Internet of Things,"
M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M. H. Rehmani, and M. S. Ali
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 seen as the last component needed to create an IoT ecosystem that is really 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 use blockchain technology to provide a decentralised, secure IoT medium.
"A review of blockchain technology in smart city applications: Research challenges and issues,"
J. Liu, Y. Liu, R. Xie, F. R. Yu, H. Tang, T. Huang, and J. Xie
The world's population has been rapidly urbanising in recent years, leading to a number of

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

economic, social, and environmental issues that have a substantial impact on people's quality of life and living circumstances. These urban issues may be resolved with the help of the "smart city" idea. The goals of smart cities are to maximise the use of public resources, provide inhabitants first-rate services, and enhance the standard of living for everyone. 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 provide 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.

"Management of synchronisation and interoperability in blockchain-based decentralised e-health systems,"

E-health systems have been widely used in recent years, mostly because of improvements in health monitoring technology and the availability of remote diagnostic services (S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty). The management of the e-health ecosystem and the security and privacy of sensitive data provide the two biggest obstacles despite the many advantages. The former is the outcome of disparate, redundant, and often duplicated data from many separate e-health service providers. The latter, however, results from private data kept in centralised systems that are vulnerable to intrusion. Blockchain is a promising technology that may be used to protect data privacy and access while offering a broad management solution for large-scale decentralised and distributed corporate systems. We provide a unified approach in this article for transferring separate, traditional e-health systems to a single blockchain-based ecosystem. We especially discuss the differences between the data formats of blockchain file databases and traditional relational databases. The answer explains how to convert and synchronise data for large-scale e-health data in a single system. The study and execution demonstrate that major gains in data storage, access control, and smooth transfer are possible.

2.1.2 ARCHITECTURE

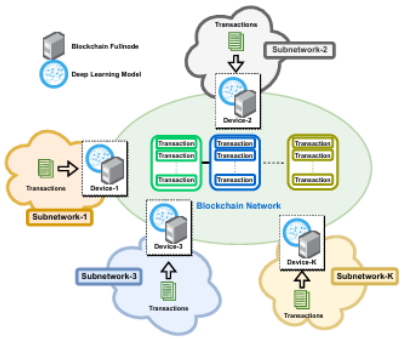


FIG.No.2.1

2.2. MODULES DESCRIPTION

2.2.1. Admin

The administrator must use a working user name and password to log in to this module. Following a successful login, one may do several tasks including seeing all users, viewing all data sets, View the Results of Cyberattack Type and Cyberattack Detection Status by Block Chain.

2.2.2. View and Authorize Users

The administrator may see a list of all registered users in this module. Here, the administrator may see the user's information, like name, email, and address, and they can also grant the user permissions.

2.2.3. User

A total of n users are present in this module. Before beginning any actions, the user needs register. Following registration, the user's information will be entered into the database.

International Journal of Engineering Research and Science & Technology

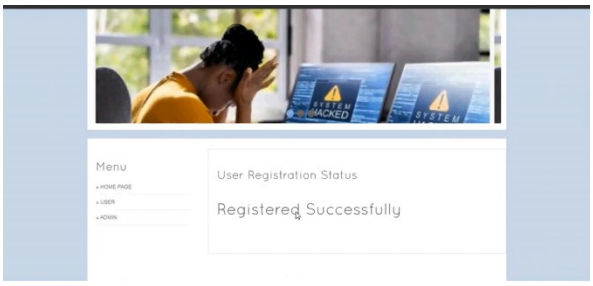
ISSN 2319-5991 www.ijerst.com

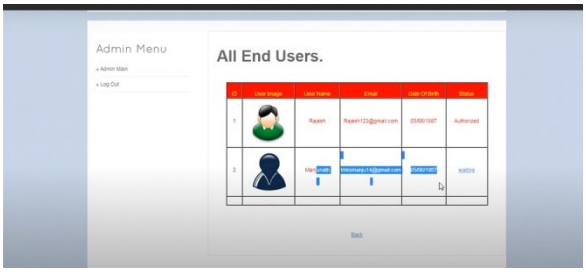
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653

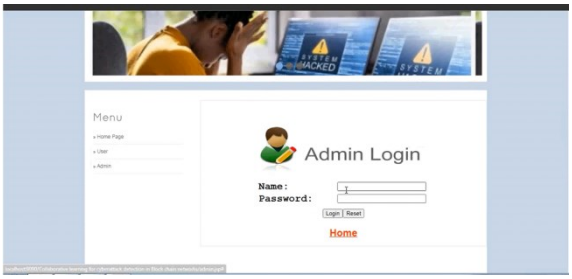
Vol. 21, Issue 2, 2025

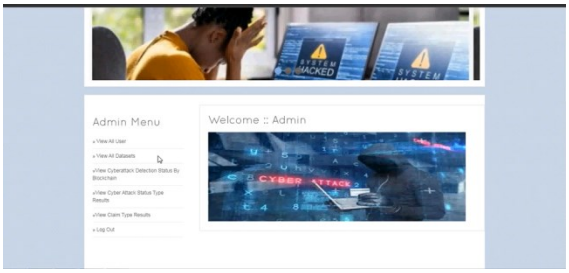
Following a successful registration, he must use his password and authorised user name to log in. The user will do many tasks after successfully logging in, including registering and logging in, seeing their profile, uploading datasets, and detecting cyberattacks. Determine the Cyberattack Detection Type Using the Block Chain Hash Code.

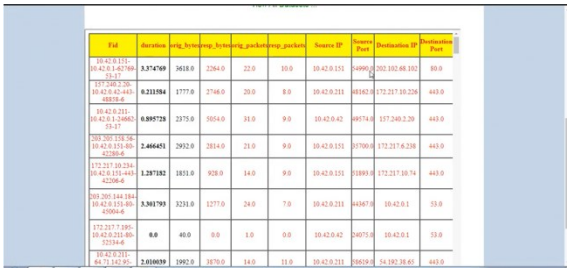
III. SCREEN SHOTS

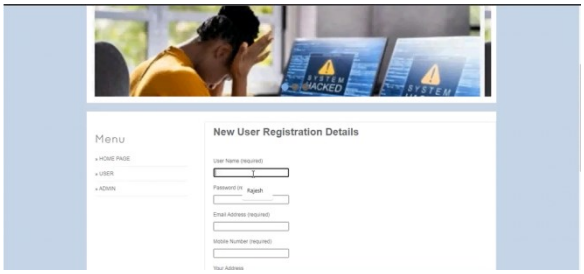


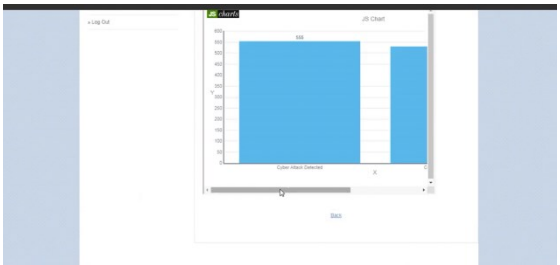


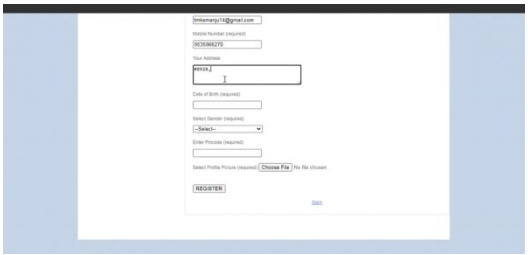










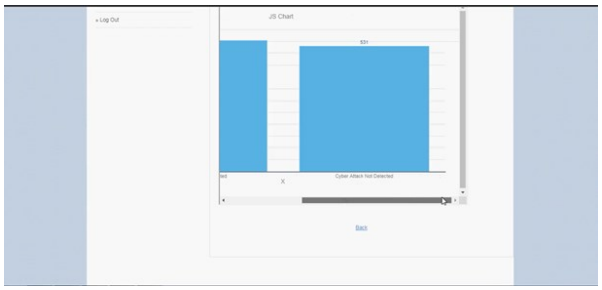


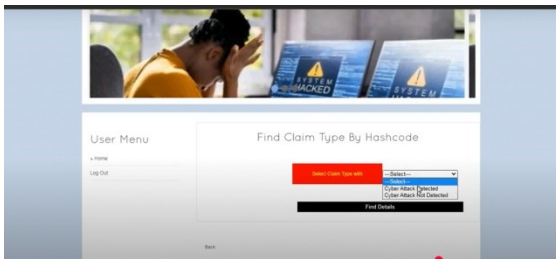
International Journal of Engineering Research and Science & Technology

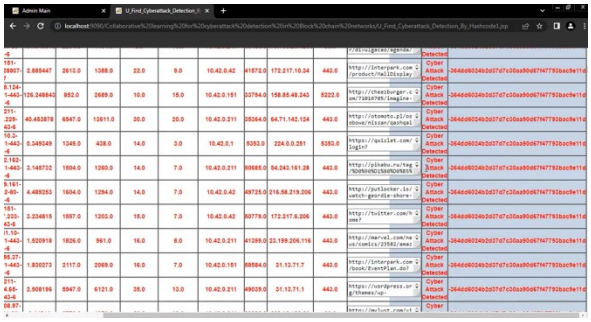
ISSN 2319-5991 www.ijerst.com

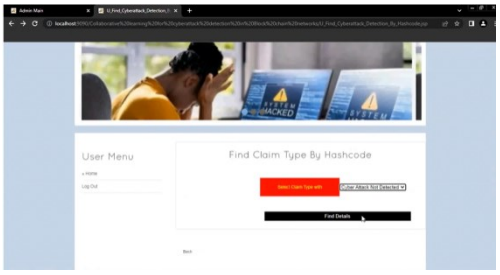
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653

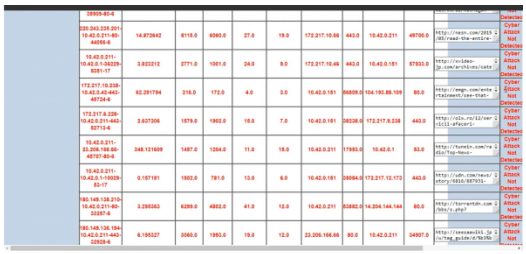
Vol. 21, Issue 2, 2025











IV. CONCLUSION

In this paper, we have put forth 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 used. 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 now been amply shown by simulation and real-time experimental data. We want to keep expanding this dataset with new attack types in the future and provide stronger defences for blockchain networks.

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

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

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 survey of blockchain technology applied to smart cities: Research issues and challenges," 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-based decentralized e-health systems," IEEE Transactions on Engineering Management, 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, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, July 2018.
[6] "The 10 Biggest Crypto Exchange Hacks In History," 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 Their Unlaundered 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 future blockchain 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, "Blockchainbased soybean 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 combined authentication and intrusion detection with data fusion in high-security mobile 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, and K. Zheng, "Attack and defence of ethereum remote apis," in 2018 IEEE Globecom 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 transaction flooding attacks against Monero," in IEEE International Conference on Blockchain 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 photovoltaic systems," 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.
[15] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," Peer-to-Peer Networking and Applications, vol. 12, no. 2,pp. 493–501, Mar. 2019.
[16] M. Idhammad, K. Afdel, and M. Belouch, "Distributed intrusion detection system for cloud environments based on data mining techniques,"Procedia Computer Science, vol. 127, pp. 35–41, Jan. 2018.
[17] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, W. Luo, and Y. Wu, "Evolutionary deep belief network for cyber-attack detection in industrial automation and control system," IEEE Transactions on Industrial Informatics,vol. 17, no. 11, pp. 7618–7627, Nov. 2021.
[18] L. Vu, V. L. Cao, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Learning latent representation for iot anomaly

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp642-653
Vol. 21, Issue 2, 2025

detection," IEEE Transactions on Cybernetics, pp. 1–14, Sep. 2020.
[19] C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, "A survey on deep transfer learning," in Int. Conf. on Artificial Neural Networks. Rhodes, Greece: Springer, Oct. 2018, pp. 270–279.
[20] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection inblockchain networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 289–318, Jan. 2023.
[21] P. Kumar, R. Kumar, G. Gupta, and R. Tripathi, "A distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT systems by leveraging fog computing," Transactions on EmergingTelecommunications Technologies, vol. 32, no. 6, pp. 1–31, June 2021.
[22] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," IEEE Internet of Things Journal, vol. 8,no. 12, pp. 9463–9472, June 2020.
[23] J. Kim, M. Nakashima, W. Fan, S. Wuthier, X. Zhou, I. Kim, and S.-Y. Chang, "Anomaly detection based on traffic monitoring for secure blockchain networking," in IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, May 2021,pp. 1–9.
[24] Z. Liu and X. Yin, "LSTM-CGAN: towards generating low-rate DDoS adversarial samples for blockchain-based wireless network detection models," IEEE Access, vol. 9, pp. 22 616–22 625, Feb. 2021.
[25] W. Cao, Y. Huang, D. Li, F. Yang, X. Jiang, and J. Yang, "A blockchain based link-flooding attack detection scheme," in IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), vol. 4, Chongqing, China, June 2021,pp. 1665–1669.