




R-GCN: a residual-gated recurrent unit convolution network model for anomaly detection in blockchain transactions

R. Rajmohan¹ · T. Ananth Kumar² · S. G. Sandhya³ · Yu-Chen Hu^{4,5} 

Received: 1 July 2023 / Revised: 3 October 2023 / Accepted: 17 December 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

The domain of deep learning has provided an exemplary paradigm for how Artificial Intelligence (AI) can be a disruptive technological paragon through Blockchain Technology (BT). Data experts have recently strived to find the quality of a dataset high enough for machine learning by an AI entity to be effective and efficient. Blockchain technology has become a special, innovative, and fashionable technological development. It also guarantees that the data is reliable and valid through its consensus process. However, new protection creates problems like data anonymity and confidentiality. Deep Learning (DL)-based blockchain data security is needed to deal with the problems mentioned above. This paper proposes an integration of the DL and BT systems, which produces highly reliable performance in enhancing data durability and dissemination. Moreover, a new convolution model called Residual-Gated recurrent unit Convolution Network (R-GCN) is proposed to analyze transactions in a blockchain-based platform using the Stochastic Gradient Boosting (SGB) technique. The proposed framework is implemented in the Ethereum environment using Anaconda and Python packages. Also, an analogy of how these models can be applied in a range of smart technologies, such as the Unmanned Aerial Vehicle (UAV), Smart Grid, healthcare, and green infrastructure, is illustrated.

Keywords Deep learning · Residual model · GRU · Convolution network · Blockchain transaction · Stochastic gradient boosting

1 Introduction

Data has become an important source of knowledge over the past few decades, creating new possibilities for real-life issues such as wireless networking, bioinformatics, agricultural fields, and Marketing through smart applications. These applications are based on stored data and integrate customer feedback into the user interface, enabling users to accomplish the intended mission more easily. It operationalizes insights, customizes customer service, optimizes consumer experiences, increases institutional performance, and makes for innovative

✉ Yu-Chen Hu
ychu@thu.edu.tw

Extended author information available on the last page of the article

business models [1]. Various smart apps, such as Amazon, Flipkart, and smart cities, make it easier for a person to work. These apps generate massive data, and storing the continuous data in the databases is an issue. Also, its connectivity often poses security issues. Blockchain technology, which has a distributed storage network, can be used to manage these problems. In the year 2008, it was invented by Satoshi Nakamoto [2] and included a time-stamped set of tamper-proof documents maintained by a distributed computer cluster. It consists of a series of blocks connected using cryptographic primitives. Immutability, decentralization, and openness are the three key pillars of blockchain technology. These three features have opened the door to a wide range of technologies, such as the nature of digital currencies and the study of their suitability in smart applications. While blockchain technology guarantees protection and confidentiality problems, some vulnerabilities have started to emerge after its introduction. The type of attacks include plurality attacks (52% attack) manipulating elections, and Sybil attacks to monitor consensus for the false identity of fake identity proof [3].

An Intrusion Detection System (IDS) is necessary to deal with the aforementioned issues since conventional approaches use a digital signature methodology to discover similar unique patterns [4]. However, new technologies such as deep learning are used to identify intrusions and attack patterns to analyze the data flow [5]. Therefore, the management of blockchain-based smart apps involves the creation of effective and efficient algorithms to process this vast volume of data. Nowadays, Deep learning is a popular technology, which has been used more than 12 times daily without noticing. DL comprises machines that learn, reflect, and function without human information or instruction. Deep learning allows machines the ability to learn without being directly coded. The basic principle is to construct an appropriate algorithm that will take the input, process the input using statistical analysis, and produce the appropriate outputs.

A huge volume of data can be processed by deep learning to select or take any data from the data driven. The communication network will have layer-wise security problems in a blockchain-based smart application. Such protection problems and malicious packets on the device layer are dealt with on the network layer [6]. Malicious packets may be used to force a false consensus on the network. Using a firewall to confirm that packets follow the protocols of security criteria could be a naive approach to this issue. However, with unseen trends to circumvent a firewall, the attacks are becoming subtler. To avoid this problem, packet header data can be evaluated in real time using deep learning models' historical data [7]. This research aims to recognize current and changing developments. Similarly, it is possible to use machine learning methods to identify destination or end-to-end side malware such as routers, mobiles, or workstations. In addition, many smart applications based on blockchain, such as Amazon and UAV, create confidentiality for the customers' purchased data. At the same time, it is very important in any smart application to provide security and safety for customer data. Blockchain technology creates trust and provides protection and guarantees for data. Deep learning methodologies are used to predict the untrusted node by comparing and analyzing the similar pattern used in the previous pattern. UAVs have a slightly different network topology when compared to the traditional blockchain. UAV uses satellite and different ground stations for communication. In UAVs, blockchain technology is mainly used to store location coordinates securely, and other vehicle-related information is retained in graph integrity [8].

Latest developments in artificial neural network-based deep learning have seen unparalleled precision in numerous functions, such as image and voice recognition, drug discovery, and cancer science gene analysis. Massive volumes of data need to be nourished into deep learning models to gain much greater precision, resulting in extremely high computational needs. However, this question can be addressed with the use of distributed

deep learning methods that have been thoroughly studied in recent years. Unfortunately, as opposed to the traditional standalone deep learning example, the privacy dilemma degrades in the sense of Distributed Deep Learning (DDL) [9].

Federated Learning (FL) is the commonly accepted method context among these current works [10]. Federated learning is also known as social learning and distributed learning. Federated learning is basically the synthesis of deep learning and distributed computing. A parameter server is one type of server in which DL performs training. The training is divided into multiple tasks. Each task should be distributed evenly on the server. For performing this task, the first data that needs to be trained will be divided and stored in the sub-server. Then, each sub-server trains the stored data by applying DL models on their local storage. The sub-server-trained data is mentioned as intermediate gradients. It will be uploaded to the parameter server. After receiving all the intermediate gradients from the sub-server, the parameter server will combine and update the deep learning model accordingly. Similarly, the process continues in the sub-server and uploads the data to the parameter server. This training process continues and repeats until it reaches a training error lower than the level stated above.

It should be noted that blockchain, derived from the decentralized currency structure, allows distrustful nodes using a consensus protocol and financial rewards to exchange a shared transaction ledger without needing a trustworthy third party. This inspires us to implement a blockchain mechanism focused on deep learning that preserves public authority and justice. Combining blockchain-powered smart contracts with deep learning data capabilities makes this dynamic feasible. While smart contracts facilitate automatic processes, deep learning can simultaneously look for anomalies, triggering human involvement when necessary. To summarize this article, the following contributions are made:

- R-GCN, a shared training platform with a reward system that invites parties to collectively engage in deep learning exemplary training and exchange the acquired local gradients.
- R-GCN protects the anonymity of native gradients and ensures the training procedure's auditability. Participants are motivated to behave honestly using reward mechanisms and transactions, particularly in gradient selection and parameter apprising, thereby preserving objectivity during collaboration training.
- Incorporated and tested the efficiency of the R-GCN prototype in terms of cipher scale, throughput, and precision of training and validation time.

The rest of the paper is organized as follows: Section 2 introduces the background work related to blockchain and deep learning in transaction security. Section 3 describes the architecture and workflow of the proposed R-GCN framework using the SGB technique. Section 4 discusses the implementation and results of the R-GCN model. Finally, Section 5 concludes the R-GCN work and implicit future deployments.

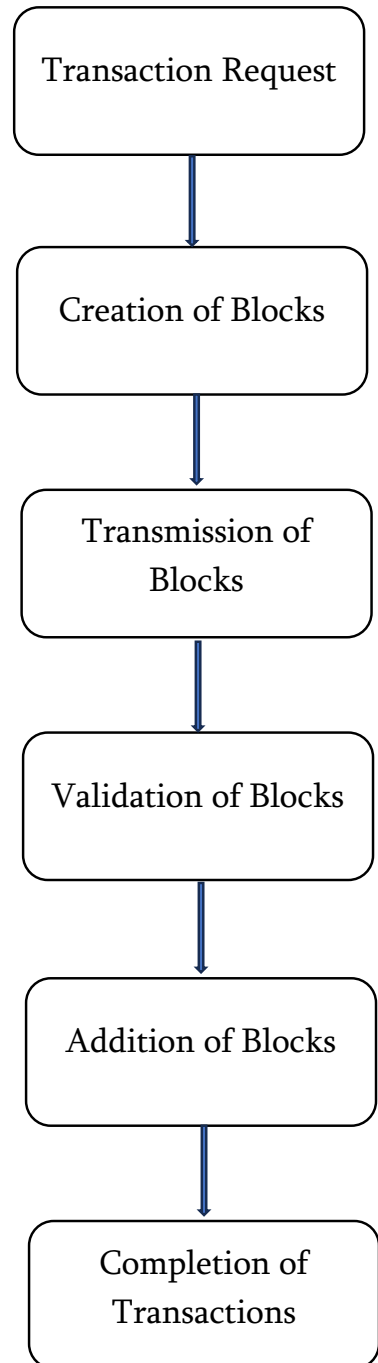
2 Related works

2.1 Blockchain models

A blockchain is a network of ledgers containing information or expertise. Satoshi Nakamoto actively and influentially launched blockchain computing in 2009 after it had already been discovered [11]. Ledger, which uses the first distributed crypto-monetary technology, has been developed. With the last block hash, every other block of the mutual ledger

network retains those details, as shown in Fig. 1. A hash is a unique arithmetic code belonging to a certain exponential element. If data within the block changes, the key hash

Fig. 1 Blockchain workflow



will also be liable for modification. The incorporation of blocks into these threat keys helps the stability of the ledger network.

The large applications of blockchain in different industries would have attracted numerous researchers to investigate the vulnerability of blockchain [12, 13]. In the past few years, multiple institutions have formed semi-governmental organizations and consortium-based blockchains, such as Hyperledger [14]. Some deep learning models [15–18] have been developed whose goals are to detect anomalies within a blockchain network using the dynamic stochastic approximation approach.

Another promising neural network model for privacy preservation is the Convolutional Neural Network (CNN) model. In CNN [19, 20], the input data is processed through a set of convolution filters or convolutional kernels, depending on the classification. These feature maps are normally used to produce useful outputs. This can be accomplished by stacking all the obtained feature maps together and performing subsampling operations on these feature maps to reduce the dimensionality of the feature maps. Most common pooling is average pooling, and causal convolution is common convolution.

2.2 Anomaly detection in blockchain transaction

The deep learning system cannot provide security or privacy for the training data, although training data is stored independently in blockchain. Researchers demonstrate that the intermediate gradients stored in the sub-server's local storage can also be used as an important message for the training data. To prove this assumption, Cheng et al. [21] demonstrated various differential security techniques for uploading data gradients. By doing that, he achieves information security along with training accuracy. Qu et al. [22] showed the implemented Generative Adversarial Network (GAN) learning for providing privacy to the parameter server. From Tramer et al. [23], The intermediate gradients were exploited to conduct a linkability attack on the sub-server because the gradients provide ample data features. Maji et al. [24] suggested using spatial domain encoding to secure information protection learning from the curiosity of a service attribute. Alabdulatif et al. [25] suggested using homomorphic encryption methods to secure data privacy from inquiring server parameters. The downside of their method is that they believed that the collaboration applicants were truthful but not interested, so their scheme could fail when certain participants were curious.

Ethereum smart contracts could be detected and classified using transaction-based analysis proposed by Teng Hu et al. [26]. A team of researchers was given access to over 10,000 smart contracts and tracked how the behavior of those contracts and the people who use them interact. They collected a dataset of smart contracts and formulated an exploratory database with a proposal for a data-slicing technique. Long Short-Term Memory (LSTM) network was used to train and test the datasets after that. A rigorous experimental analysis demonstrates that their technique can differentiate between various types of contracts and be applied to finding malignant ones.

Dorcas et al. [27] defined architectural anomaly detection in flexible multilayer networks. They hypothesized that abnormalities in the inherent blockchain transaction graph will express abnormal structures of system shape properties. Finally, they used persistent clique homology on graphs to track the evolution of network shape and thus detect changes in network topology and geometry. The layered perseverance chart is a new multilayer network persistence overview that is stable under input data disturbance. They tested the topological anomaly detection framework on the Ethereum Blockchain

and the Ripple Credit Network. The authors [28] proposed two Phishing Detection Frameworks (PDF) based on feature learning and transaction record mangling. According to the results, the phishing detection framework outperforms existing phishing detection frameworks and needs to be improved against malware activity. A Self-supervised Incremental Deep Graph Learning (SIEGE) model for spoofing scam identification on Ethereum was proposed by Shucheng Li et al. [29].

The common architecture for data storage in the blockchain-based system is shown in Fig. 2. First, extensive recording for consumer data protection preservation is not

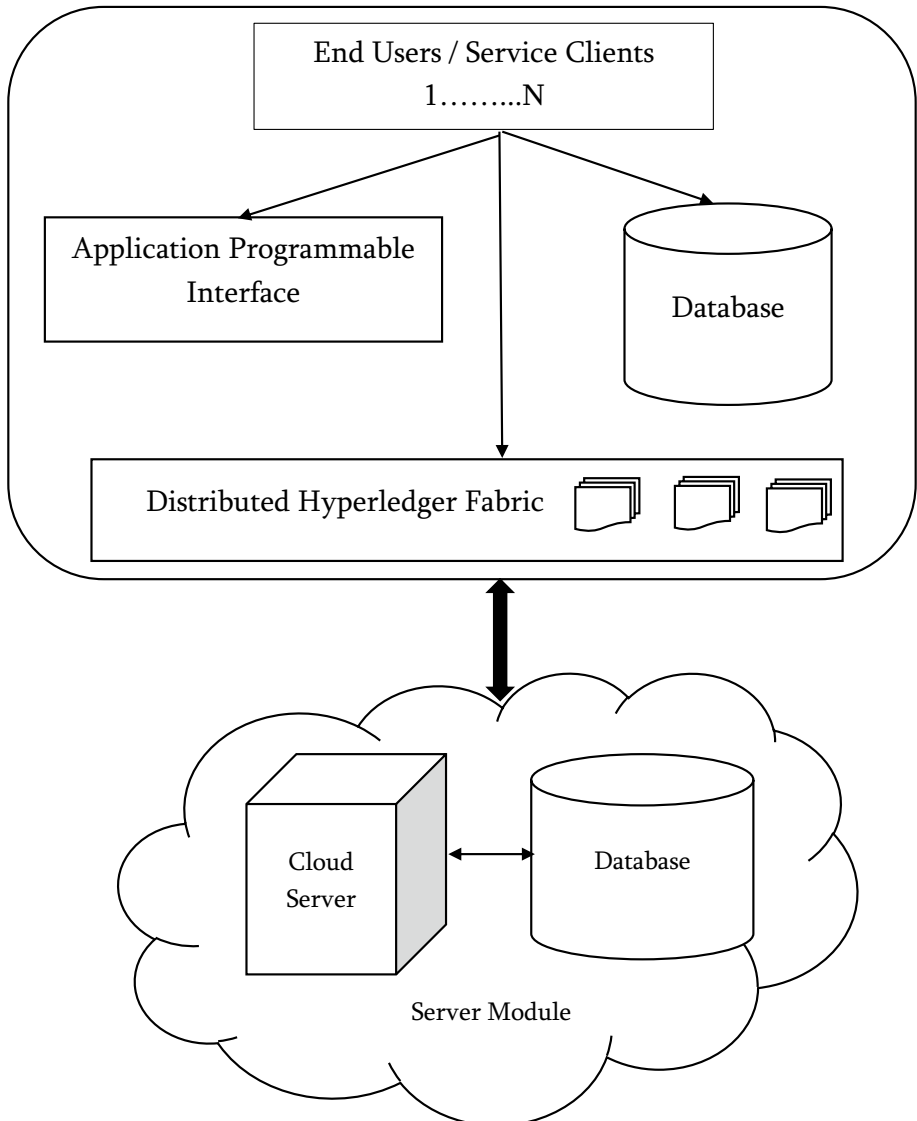


Fig. 2 Blockchain architecture for data transaction

permissible here. Secondly, it helps to substantially reduce the need for transactions. And other metadata is stored in the blockchain. In addition, data pointers stored in the block can be connected to the raw data position in the data integrity off-chain database. However, maintaining this confidential data makes it difficult to completely trust third parties. Meanwhile, decentralization can also contradict the notion. The authors in [30] used byte-code, hybrid class, and hybrid label classification methods to distinguish smart contract security issues such as reentrancy, denial-of-service, and payment source.

Several survey papers have been released by various canvassers on the various facets of DL acceptance of blockchain-centered insolent solicitations [31–36]. As per the research, most studies concentrated on regions, sectors, or implementations where deep learning and blockchain are needed. The suggested survey includes all the basic dimensions of BT-based technologies to be added to DL, such as interference detection. An analysis was published to explain what way to detect interference by blockchain. The authors reduce confidence issues by creating a collective IDS using smart contracts.

Furthermore, a work polled Bitcoin on confidentiality and integrity issues. They address different types of attacks, such as dual expense attacks, vulnerability breaches on the client side, and attacks on mining pools. Chancellor et al. [37] explore concrete DL strategies and deliberate the behavior of precise social problems such as human transferring and opioid sales by cryptocurrencies to resolve the problems. Then, using DL tools, Zhong et al. [38] explored malware detection. Malware characteristics have been explored extensively, and a detailed taxonomy has been recommended. A detailed analysis was undertaken by Marchetto et al. [39] on blockchain applications.

3 The proposed Residual-GRU Convolution Network (R-GCN) architecture

The existing paradigm for exchanges in the transaction segments is addressed, and we proposed the R-GCN model, a stable and decentralized platform for blockchain transactions that preserves privacy. By implementing incentive structures and transactional analysis, R-GCN ensures collective teaching. Information security and accountability were ensured with encryption protocols during the joint learning phase. The R-GCN is a stable and decentralized system built on the blockchain and cryptographic primitives for DDL to maintain anonymity, which will provide privacy, accessibility of computations, and inducements for the sub-server to engage in collective training. Figure 3 shows the proposed anomaly detection using R-GCN and SGB models.

In specific, R-GCN is secure because it inherits the DDL model. On the left is the conventional distributed training system, whereas the model's right side is the R-GCN communication scheme. Here, in R-GCN, the Marketing and processing agreements are intelligent agreements that jointly commit to secure learning, whereby T_x relates to contracts. By initiating transactions, aggregate local intermediate gradients from untrusted parties while local preparation and parameter updating are carried out to process the transaction.

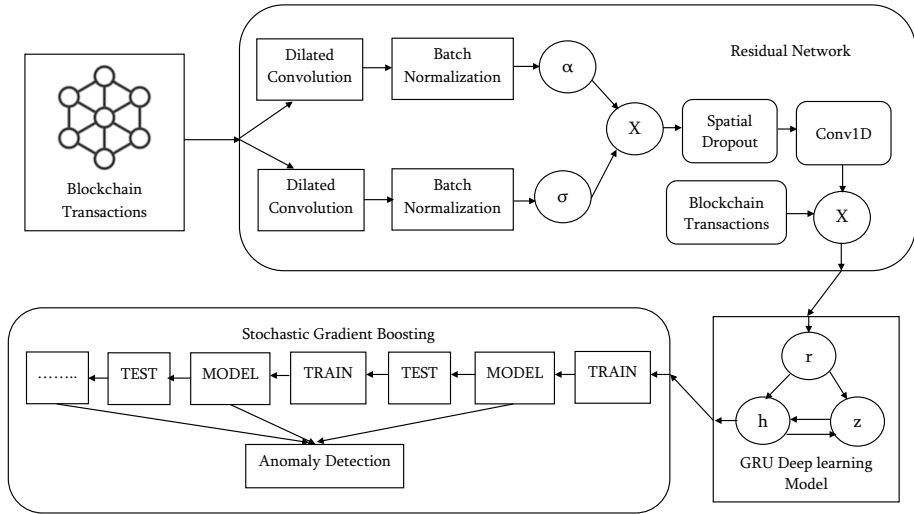


Fig. 3 The proposed anomaly detection model

3.1 R-GCN architecture

Since the blockchain transactions change over time, we employed the residual Gated Recurrent Unit (GRU) convolution network model to solve our problem. R-GCN is a type of Graph Neural Networks (GNN) that can deal with structured data from time series. R-GCN predicts tasks by considering both spatial-temporal characteristics depending on data from the past. This model is made up of RN and GRU models. Residual Network (RN) is a structure that uses random convolutions and dilations to adapt to time series data with substantial receptive areas and transitivity. RN deploys a multi-layer perceptual neural network that uses adjacency and feature matrix to predict the time series. For each layer in RN, the rule for transforming information from one layer to the next is represented in Eq. (1).

$$H_l^{i+1} = \varnothing(\ddot{D}_n \cdot \ddot{A}_m \cdot H_l^i \cdot W_l^i) \quad (1)$$

where, H_l^{i+1} represents the current convolution layer, \varnothing denotes the activation function, \ddot{D}_n signifies the matrix of normalized degree, \ddot{A}_m is the adjacency matrix, H_l^i denotes the previous convolution layer and W_l^i represents the weight matrix of the previous convolution layer.

GRU is a form of Recurrent Neural Network (RNN) model that accounts for data's temporal dependence. RNN is a standard option for handling sequential data. Nonetheless, it cannot identify long-term connections. Consequently, LSTM and GRU are the best deep learning models for defining prolonged relationships. GRU was selected over LSTM due to its faster training process. In addition, GRU is equipped with a method for learning long-term connections. Specifically, there are three gates: the reset gate, which determines how much knowledge from the previous timestamp to disregard, the update gate, which determines how much knowledge to transfer into the present timestamp. And the memory gate, which saves the storage in the present timestamp. The R-GCN unit is denoted by the preceding equations:

$$U_t = \sigma(W_U[R_b, O_{t-1}] + B_u) \quad (2)$$

$$R_t = \sigma(W_R[R_b, O_{t-1}] + B_R) \quad (3)$$

$$M_t = \text{Tanh}(W_M[R_b, R_t * O_{t-1}] + B_M) \quad (4)$$

$$O_t = [U_t * O_{t-1} + (1 - U_t) * C_t] \quad (5)$$

Here R_b represents the functioning of the residual block, O_t is the output at time t , U_t denotes the update gate, R_t denotes the reset gate, M_t denotes the memory gate, B refers to the bias, σ and Tanh denotes the activation function. The R-GCN model first retrieves the structural features from the transactional data using RN for each convolution. Then, it uses GRU to extract the spatial-temporal features at the present timestamp and knowledge from preceding timestamps to anticipate the output at the subsequent timestamp. This is done so that the model can capture both the temporal and spatial dependencies at the same time. The predicted values are designated residuals and provided as input to the SGB model for anomaly detection.

3.2 Layered communication

To make blockchain transactions smarter, DL's learning features can be extended to blockchain based applications. Protection of the distributed ledger can be increased using deep learning. Deep learning can also be used to maximize the time required to achieve consensus by providing improved routes for data exchange. Furthermore, it offers an opportunity to build enhanced models by making benefits of the distributed framework of blockchain technology.

As seen in Fig. 4, it exhibits the R-GCN framework with deep learning implementation for smart applications based on blockchain technology. Here, the smart program gathers information from multiple databases, such as cameras, smart machines, and IoT devices. As part of smart apps, data obtained from these sensors is analyzed. The blockchain acts as an important part of this smart software. Then, deep learning can be added to the data to interpret and estimate this application. We could store the database sets carried by deep learning models on a network of blockchains. This eliminates data faults such as repetition, lost meaning of data, errors, and noise.

The R-GCN model incorporates blockchain and deep learning features. Blockchain is based on data, which may remove data-related problems in deep learning models. The benefits of the proposed framework are listed below:

- User authentication as a valid user of the blockchain network for requesting or executing some transaction.
- A high degree of protection and trust is provided by blockchain technology.
- To ensure that the terms and conditions previously negotiated are maintained, blockchain incorporates public deep learning models into smart contracts.
- Blockchain technology helps to enforce an incentive-based scheme efficiently while enabling consumers/clients to subsidize data. The enormous amount of data will boost the efficiency of the deep learning model.
- On deep learning models with a minimum charge and off-chain, BT's on-chain environment can be enhanced directly on a specific device without any cost.
- Effective consumer/client information inputs can exist; such data are periodically measured, and promotions can be accessed by consumers.

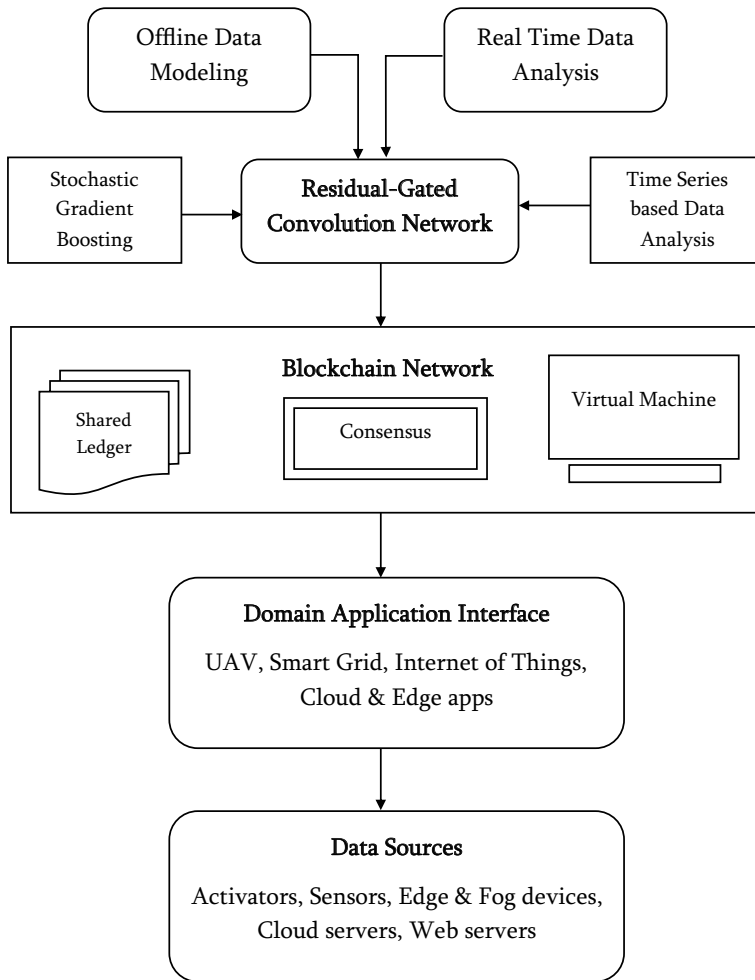


Fig. 4 R-GCN communication

3.3 Transaction data model

Transactions are around a secure electronic data packet that carries a notification that must be received through Financial Markets (FM). Apart from the previously stated receiver, exchanges at Hyper ledger fabric often include a unique identifier representing the sender, the quantity of Ether indigenous encryption that will be sent from the transmitter to the receiver, and an external memory layer that could be used where the receiver is an FM. Each contract should identify a cap specifying how many cryptographic steps can be taken in the process execution. The transaction is represented in native cryptographic bitcoin to avoid online reservation threats on blockchain technology. The costlier the payment algorithmically, and the more information is analyzed in a system as part of that deal, the more steps are taken for an effective payment.

Furthermore, the amount the recipient is prepared to pay for each measurement phase should be entered into the contract [40]. Users sign or post specialized apps or token transfers. Many forms of portfolios exist, such as portfolios for documents, smartphone payment or digital portfolios, portfolios for equipment, and wallets for desks. Each wallet class has the consistent theme that they all have a digital signature for the user, which is necessary for decentralized applications to execute actions (i.e., transactions). A graphical interface with a distributed network carries out an electronic money signature using a software wallet that maintains a users' personal key encoded with a login in the specific server system.

The background of the payment of one account is the statistical analysis records, which gather information sequentially along a timescale. Many experiments on deviations in macroeconomic variables have been conducted and extensively analyzed. The only way to analyze standard statistical analysis approaches is to vary observational data and not to mix frequency and volume. The use of machine learning, more precisely CNN, RNN, LSTM, and GRU variants, seems to be another method to examine a sequence [41].

The downside of these Resnet methods is that supervised learning needs a great amount of information, which therefore takes time. Because each address' transaction information is reduced, the irregular recognition method can be built with RNN for regression analysis. With standard approaches of neural approaches, the difficulty is to prevent multiple regression analysis due to the sequence of time series results. Feature extraction is the problem. The functions to be used in conventional intrusion identification systems must then be derived from the temporal data. Thus, the Expanded Temporary Convolution Network with a stochastic gradient mechanism is provided for statistical analysis.

The gathered findings are used in each account: timing stamps of payment and the interest of payment with its respective dollar value at the time of payment. Each domain name has several past exchanges. The quantile regression aggregation approach is used in the system, where the additional innovations were derived from the statistical methods. The period sliding window extracted function is a method in which data from the first data in phases of size S_w are sequentially evaluated and specified as the number of observations in the temporal series. R_w , which is the number of dimensions in a frame, is the duration of the revolving frame. Tables 1 and 2 display the simple method for removing features over the last bitcoin payment.

The growing period frame introduces a random series that measures frequent pattern agglomerations. In this study, the scale of the period window m was specified as the timeline, and the amount of payment process was not calculated. Phase H was also known as a single payment. As every ledger account may have specific transaction trends and our investigation aimed to conduct a personalized transaction identification, various distinct timelines are being used as periods scale h : 6 hours, 12 hours, 1 day, 3 days, 1 week, and

Table 1 Transaction history

ID Index of transaction	Duration (Year-2022)	Ether value
Ox96vbvb3v548df5ddf6	Dec 3 10.05 AM	0.000589621
Ox89cgf6g4g483das13s	Dec 3 14.15 PM	0.000987253
Ox5ssffg1c2 × 2e62bui22	Dec 3 22.20 PM	0.001985642
Ox12asettbc235a689qa1	Dec 4 10.15 AM	0.002876543
Ox36sdf145rt87shb2d53	Dec 6 10.30 AM	0.000978654
Ox1asrv12m6dr79s5w82	Dec 10 10.05 AM	0.000842365
Oxfh2d48zaw74v5c9c321	Dec 27 11.00 AM	0.001452897

Table 2 Feature extraction

ID index of transaction	Ox1asrv12m6dr79s5w82
Duration	Dec 10 10.05 AM
Ether value	0.000842365
\$ price value	1.07
U_1V_1	0.000145238
U_1V_2	0.174258932
U_2V_1	0.007845823
U_2V_2	0.000874523

2 weeks. The scale of the period frame is also not set since the payment varies through the frames. The purpose of our study is not to establish which of the other timescales are typically most important but to create a specific process that sets the required timeline for each identifier.

The combined parameters employed on the frames for payments are average, variance, confidence interval, total, and counting of the payments in the frame. Collecting payment numbers allows the regression model to be translated into Tables 1 and 2 and conventional suspicious identification to be used. The T_w -time variations and the agglomeration mechanism for the entire range $\{1 \dots p\} \cup \{1 \dots q\}$, are referred to as the U_pV_q mixture. Quality V_n is the number of timelines used in feature maps, and V_k is the number of added features in the frame range used. For each operation, the feature maps are then the U_pV_q variations of all timelines W_h and all functionality fag , respectively, culminating in relation to the initial dollar value of the payment process feature vectors.

3.4 Anomaly detection algorithm

This article discusses possible methods by which blockchain transactions could be automated and customized. Moreover, the history of customized anomaly detection for distributed ledgers and customized anomalous detection systems for decentralized transactions is illustrated. Also explain how our current technique makes an automated analysis and digital signature of decentralized applications instead of the actual manual approach to the same use case as previously defined. Until the anomaly detection system is created for one specific address, sample data must be available to display the transaction patterns for that particular address. Here, the number of the minimum transactions required is set to 50, which was proven to be sufficient experimentally to reveal fundamental transaction patterns. This is one of the criteria for future studies, but it is not within the scope of this research. The feature extraction method in R-GCN model, will begin its execution after the first 50 transactions are realized as historical data. The anomaly’s monitoring system helps us in training the model for detecting anomalies in blockchain transactions. This system is used to evaluate any payment and classify them as normal or abnormal transaction. Algorithm 1 demonstrates the process of anomaly detection using stochastic gradient boosting algorithm.

Input: Input Set $R = \{ \{T^w, U_p V_q, V^n, V^k, f_{ag} \} \}_{k=1}^r$,

Loss Function $L(\alpha, R)$

T^w - Period of data availability

$U_p V_q$ - Combination data values between period p and q

V^n - Size of the period window n

V^k - Size of the period window k

f_{ag} - Aggregate function

Method: SGB-based R-GCN

Output: $O_k(R)$ Outliers in the transaction ID.

Step 1: **Check** *TIME PERIODS* are *EQUAL*:

Step 2: **If** *EQUAL* neglect the transaction analysis.

Step 3: **End If**

Step 4: **End Check**

Step 5: **If** the *VALUES* are different, **THEN** feature analysis is initiated:

Step 6: **Define** *RESIDUALS* using *R-GCN*.

Step 7: **End If**

Step 8: **Check** for anomaly values in the derived features:

1. *Initialize the SGB model with a constant value*

$$S_y = \operatorname{argmin}_{k=1}^r L(\alpha, R)$$

2. *For k=1 to r*

a. *Compute the SGB residuals*

$$r_{i=1 \text{ to } m} = - \left[\frac{\partial L(\alpha, S(y_k))}{\partial S(y_k)} \right]_{S_y = S_{r-1}(k)}$$

b. *Train the residuals using the set $\{(R, r_i)\}_{k=1}^r$*

c. *Compute the multiplier α*

$$\alpha_m = \operatorname{argmin}_{k=1}^r L(\alpha, R, O_k(R) + \alpha h_m(R))$$

d. *Update the R-GCN model*

$$O_k(R) = O_{k-1}(R) + \alpha_m h_m(R)$$

3. *Output is derived as $O_k(R)$*

Step 10: **End Check**

Step 11: **If** analogous features **Found**

Step 12: **Return** the corresponding transaction ID.

Step 13: **End If**

Step 14: **End.**

Algorithm 1 Anomaly detection using SGB

Recently, SGB has come to attention due to its speed and accuracy of prediction, especially with massive and complicated data [42]. It is based upon the belief that when subsequent models are combined, they produce the greatest available model. This model's key concept is establishing the outcome targets to minimize errors. When determining the objective result for each scenario in the information, the accuracy of how that case's prediction changes the prediction error has a major impact. The new model for the proposed framework is built in the trajectory of the gradient descent of the previous transaction. The fundamental characteristic of SGB is to reduce the loss function from classification to the real function during training. Anomaly detection is to be able to differentiate between anomalies. In our framework, SGB is used to overfit a training dataset quickly. Finally, it can benefit from regularization methods that penalize various parts of the algorithm and generally improve the performance of the algorithm by reducing overfitting.

It was a process of evaluating the effectiveness of the proposed approach and not finding optimal settings. We only used one method of detecting anomalies—the temporal convolution network method [43], which isolates each process and separates it into standard transactions and outliers. The nature of vulnerability scanning issues through labeling instances is such that the contacts are unfounded. In other words, the error tracking framework is often unable to determine whether a phenomenon was detected correctly. This is often referred to as innovation recognition. Therefore, an unregulated vulnerability scanning service on a statistical analysis map is illustrated that indicates the outlier payments that were identified.

4 Results and discussions

Our investigation into the suggested transaction security technique includes real-time trials and simulations to gauge the effectiveness of the new approach based on the transaction offloading process. The real-time implementation includes the Ganache tool for creating and manipulating transactions. The job offloading process is the toolset for evaluating the proposed R-GCN blockchain network. In order to achieve high transfer speeds and low latency computation, we implemented a Ganache [44] Ethereum blockchain network on the Lambda Edge1 service [45]. The processing unit for the edge service was built in Fedora 34 virtual machine running at 3.06 GHz. A Samsung Android phone is employed with specifications like version 11.0, Mediatek Dimensity 700 processor, 8GB of RAM, 128GB of expandable storage, and a 5000mAh battery to evaluate the suggested offloading system. Mobile devices use IEEE 802.11 g Wi-Fi wireless communication to connect to the edge cloud computing on the wireless network. Installing a blockchain client turned the cell phone into a miner node.

4.1 Transaction offloading performance analysis

The proposed anomalous detection method for transactions utilizes 6 Ethereum addresses created by using the Ganache tool, and their characteristics are described in Table 3. The transactions of the addresses were performed by the Ethereum public main network on 2 December 2022. The transactions were executed for the onset of 24 h and randomly distributed for 2 weeks. Each block from ID 4,258,976 is analyzed to find appropriate unique addresses to fulfill the following criteria. The address in a block must be managed by a private key with at least 4k of incoming transactions, which involve transferring any amount of cryptocurrency.

Table 3 Timeline of feature extraction

Time frame	Ranking of transaction				
	Minimum time period	Maximum time period	Mean value	Median value	Std. deviation
6 h	1	2	1.4	0.7	1.3754
12 h	1	4	2.2	1.1	0.9872
1 Day	2	8	3.2	1.6	1.0869
3 Day	3	9	4.7	2.4	1.2871
1 Week	4	10	5.8	2.9	1.6542
2 Week	5	9	7.6	3.8	1.7314

The following were other settings of the procedures used in the experiment. The blockchain network is simulated using a Ganache drizzle server, and various numbers of mobile users (miners) are engaged to process data. $T_i = 5,000$ timeslots are used in the simulation, with each timeslot lasting one second. For each transaction, we postulate that the size of the data tasks produced is widely dispersed between 100 and 200 KB. Because the data in the blockchain merely contains metadata, this is a real possibility in our circumstances. Assume the latency tolerance of 15s and throughput of X of 25,000 CPU cycles/bit locally. When using the Ganache server, the power utilization coefficient and constant circuit voltage are set at 15–27 and 961 W, and the carrier boost coefficient is 0.7. In the R-GCN network, the learning rate is assumed to be 0.001. The SGB algorithm was used and realized with a gradient function to evaluate the feature importance. Then, in the hidden layers, we use Adam as the activation function, but in the output layer, we use the SoftMax activation function to loosen the offloading decision variables. We focused on three parameters to assess the transaction offloading performance of mobile blockchain.

- Transaction offloading delay.
- Power energy consumption.
- Privacy level of transaction execution.

The system efficiency was tested using two different scenarios: local execution and offloading to an edge computing service for IoT data processing. This scenario has two possible outcomes. First, transaction data is processed locally on the mobile device. In the second case, the transaction data is sent to the fog computing platform, where it will be processed. The proposed approach was tested on a variety of sensor data files ranging in size from 100 KB to 200 KB.

Two performance measures were used to examine the implementation's outcomes: processing time and energy usage. When a transaction is offloaded to a fog cloud server, the processing time comprises execution time and offloading and downloading time. Figure 5 shows that for each blockchain transactional data file size, the average processing time for local computation is greater than the average processing time for edge computing. While computing a 100 KB file, the offloading technique can save as much as 28% of the time, and when computing a 200 KB file, the offloading scheme can save as much as 37% of the time.

In the blockchain data transaction offloading process, our R-GCN model utilizes less energy since the resource-intensive computing tasks are moved to fog servers, as shown in

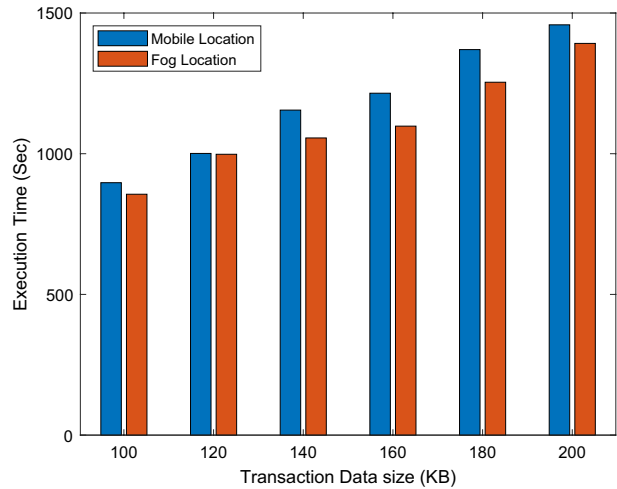
Fig. 5 Average processing time

Fig. 6. For instance, unloading a 100 KB file uses 12% less energy than doing the computation on demand. In our case, the offloading process becomes more energy-efficient as data sizes grow. Our R-GCN-based transaction offloading schemes save 14.7% and 18.5% on average when running a 100 KB file and a 200 KB file correspondingly.

4.2 Convergence cost analysis

Next, the convergence performance of our R-GCN model is evaluated and compared with existing algorithms like LSTM [46], Transfer learning-based multi-adversarial detection (TAD) [47], and SIEGE by assuming the learning factor as 0.001 throughout the training process. A single-user scenario was used in the simulations. The single-user model has just one miner, and the number of transactions at each miner can be changed ($M=5 \sim 14$). Each

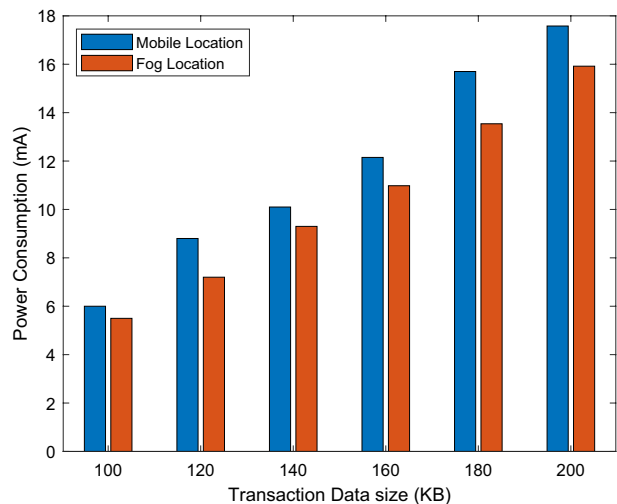
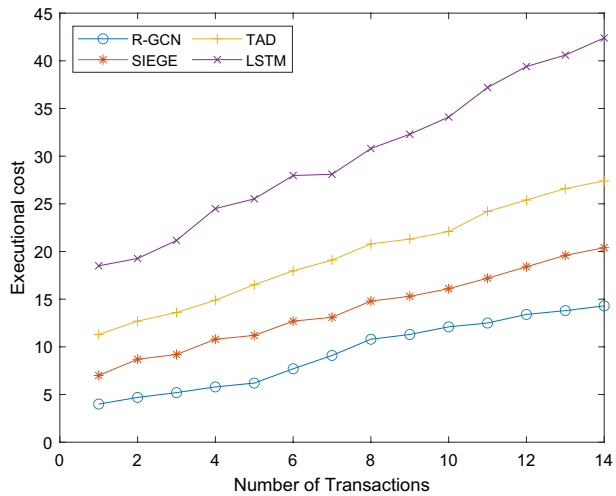
Fig. 6 Power consumption

Fig. 7 Convergence cost analysis

transaction has a different size, ranging from 100 KB to 200 KB. Figure 7 depicts the convergence simulation results.

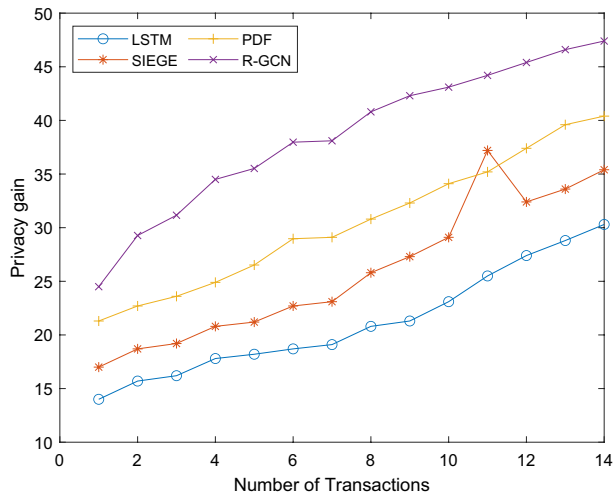
As the number of transactions (T) grows, so does the cost of five different ways since the amount of transaction data on the blockchain network is expanding. Using the TAD method, transaction costs rise from 18 at $T=5$ to 38 at $T=14$, whereas the SIEGE strategy likewise costs 20 at $T=14$. It is also more expensive to run the LSTM algorithm because it consumes more energy, reaching 45 at $T=14$. The rationale for this finding is that as the number of data processing jobs increases, the mobile miner's computational capability decreases, making it less able to provide mining services for all those tasks. Because fresh blockchain transactions must wait in the buffer of local devices before being processed, mining becomes more expensive. In addition, the increased price is due to a longer processing time and higher power usage. The suggested R-GCN system achieves the best performance with the lowest cost of 17 at $T=14$, including all data processing activities.

4.3 Privacy performance analysis

As shown in Fig. 8, we then evaluate how well the proposed R-GCN framework performs on the privacy metric. We examine how well our R-GCN system protects privacy compared to the TAD, PDF, and SIEGE approaches.

Figure 8 shows that when transaction data increases from 100 KB to 200 KB in each time slot for all strategies, the privacy level of the blockchain miner decreases. However, the R-GCN approach offers the best privacy protection compared to the other methods. For example, the suggested R-GCN scheme achieves 6.7%, 8.4%, and 13.5% higher privacy levels than the TAD, PDF, and SIEGE methods, respectively, when the mobile user mines 100 KB of blockchain transactions. Furthermore, when mining 150 KB of blockchain transactions, the R-GCN technique still has superior privacy performance, outperforming the SIEGE approach by 7.4%, the PDF approach by 9.5%, and the TAD approach by 17.8%.

Fig. 8 Privacy gain



4.4 Transaction analysis

The performance of the transaction execution is analyzed using metrics such as Minimum Time Period, Maximum Time Period, Mean Value, Median Value and Standard Deviation Value. These metrics enable us to understand the timelines of various transactions and thus enhance the overall throughput. Figure 9 depicts the creation of blockchain transactions.

The important factors were evaluated using the SGB algorithm, which is identical to the transaction data input in the R-GCN anomaly detection method, and the anomaly labels output by the SGB are the target values. The corresponding SGB model consisted of the [0,1] ranges of characteristics, of which the greater the number is, the better. As there are different aggregations on each window, the value has been summed up for a single window to calculate each address’s significant points of time. The simulated outcomes of the

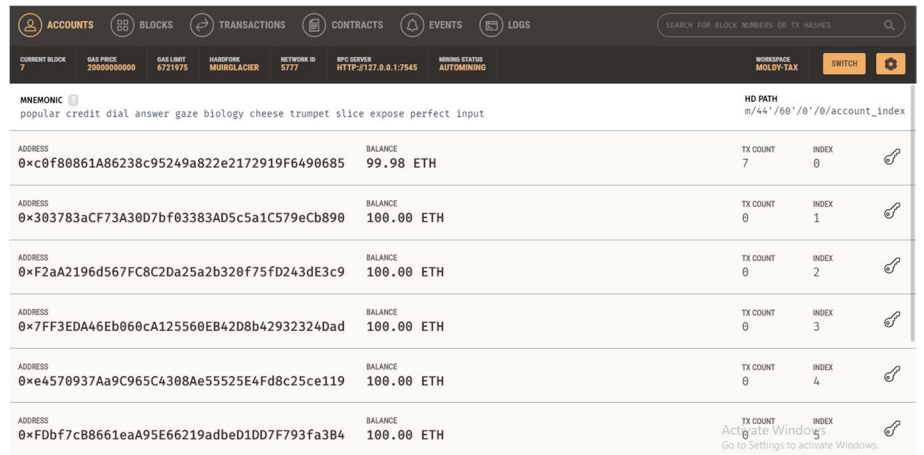


Fig. 9 Blockchain transactions

recommended framework are exhibited as a box chart in Fig. 10 and bar charts in Fig. 11, where the bar length denotes the summation of key factors for that period; the outcomes are also shown in Table 1.

The results presented in Fig. 12 show that across all five addresses in our experiment, there is no clear pattern of the most relevant timelines. The address beginning with 0x12 is clearly different from other addresses because the longer period of timelines is more essential than other addresses, where timelines dominate factors of relevance in less than one day. Table 1 results display these time frames' lowest, highest, and midrange ranks and the normal ranking deviation. The most significant feature for the five addresses examined is 6 h; the average rating is the lowest (1.4). This is followed by the day before the time frames (mean range of 3.2) and the week (mean rank of 58) (mean rank of 4.2). Standard deviations of these ranks are reasonably high (at least 0.98 for an hour and at most 1.73 for a single transaction), suggesting that there is no clear consensus. To conclude, using an R-GCN-based SGB model for anomaly methods of transaction detection is acceptable since the inter-address differences are important for addressing anomalous transaction detection, which is explicitly tailored to patterns for each address transaction operation.

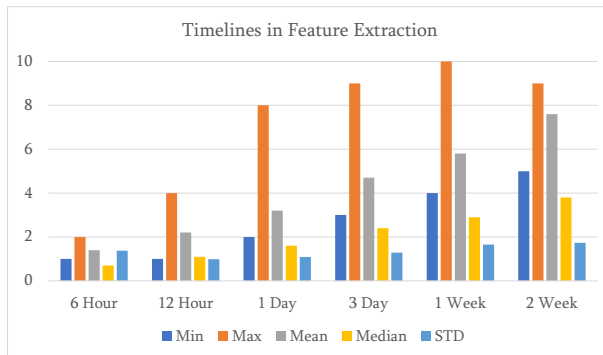
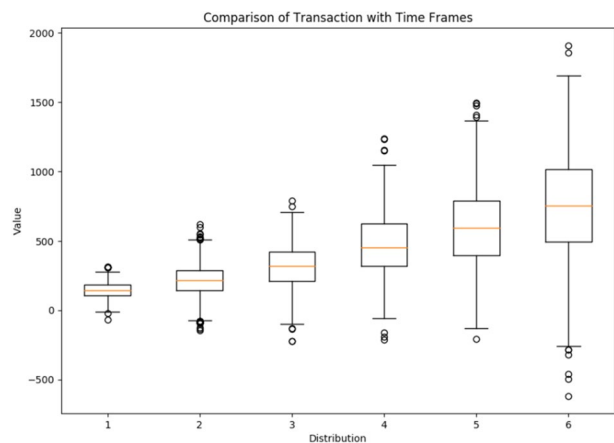


Fig. 10 Feature analysis of transaction in different timelines

Fig. 11 Transaction timelines



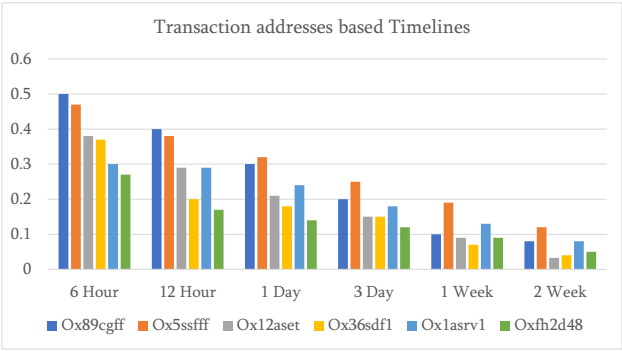


Fig. 12 Address based feature analysis

Table 4 Comparison of execution time

Methods	LSTM	TAD	PDF	SEIGE	Proposed R-GCN
Time complexity	$O(n^2)$	$O \log(n)$	$O \log(n)$	$O \log(n)$	$O \log(n)$
Duration	311 s	275s	256s	208 s	186 s

The performance of the proposed framework outperformed the existing ones based on three determinant inferences in the methodology. First and foremost, the suggested scheme focuses on removing inconsequential identities prior to applying those to the deep learning model, which is an essential step in the process. For the second time, our methodology uses blockchain-based cryptographic primitives for DDL to maintain anonymity, which will provide privacy and accessibility of computations. Third, considering the gradient boosting algorithm for parameter selection reduces objectivity loss during collaborative training, and the system can be influenced to produce an appropriate output class.

Also noteworthy is that, compared to existing algorithms, the proposed anomaly detection algorithm achieves more remarkable outcomes while simultaneously decreasing the time complexity by relying on a DL structure. Furthermore, as shown in Table 4, the scheme is significantly faster at detecting anomalies than the models under consideration. Despite the excellent performance achieved by the suggested strategy, our model has constraints when confronted with a larger number of transactions in a delayed timeline. This is due to an increase in the data computation period, which reduces the off-time period execution.

5 Conclusion

This study offers an extended temporal convolution network-based blockchain architecture for improving transaction security and specifics on blockchain technology and deep learning. With this architecture, a data analysis framework for DL-BT can be designed and deployed quickly and easily. There was a discussion of some of the current methods and their shortcomings. The blockchain transactions were analyzed using the SGB algorithm

to find outliers, which were then categorized using the R-GCN model. Ethereum and the Anaconda package are the implementation platforms realized for simulating the proposed framework. The extracted transaction features depict no clear consensus in the available transactions. The performance of the proposed system is measured in terms of throughput, training time, and validation time. The transactions were executed for the onset of 24 h and randomly distributed for 2 weeks.

The simulation results reveal that the proposed model prevents the execution of analogous entities in the transactions. Additionally, no anomalies were encountered in the proposed framework because of the blockchain's integration with the expanded temporal convolution network. The proposed work has been applied in intelligent applications at the application layer level. But the R-GCN model has not addressed centralized control, adversarial attacks, security, and privacy measures at the layer level. Extensive research can extend the model to cloud and edge layers to provide accurate data analysis at low latency. Next, private blockchain platforms ensure data privacy through private channels and access control policies. However, public blockchain platforms are prone to data privacy leakage problems because they have a zero-access control policy. Therefore, public blockchain platforms can realize R-GCN model for achieving data privacy and security. Finally, the efficiency of blockchain-based applications is highly improved by increasing the size of the blockchain network. Hence, the proposed R-GCN approaches can be employed for compressing the data and minimizing the redundant data in future.

Funding The authors declare that they do not have any funding or grant for the manuscript.

Data availability The datasets generated during and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Declarations

Ethical approval No animals were involved in this study. All applicable international, national, and/or institutional guidelines for the care and use of animals were followed.

Conflict of interest The authors declare that they do not have any conflict of interest that influences the work reported in this paper.

References

1. Yang R, Yu FR, Si P, Yang Z, Zhang Y (2019) Integrated blockchain and edge computing systems: a survey, some research issues and challenges. *IEEE Commun Surv Tutor* 21(2):1508–1532
2. Nakamoto S (2008) Re: Bitcoin P2P e-cash paper. *Crypt Mailing List* 1–2
3. Kiania K, Jameii SM, Rahmani AM (2023) Blockchain-based privacy and security preserving in electronic health: a systematic review. *Multimed Tools Appl* 82:28493–28519. <https://doi.org/10.1007/s11042-023-14488-w>
4. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J (2019) Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity* 2(1):1–22
5. Liu H (2019) Machine learning and deep learning methods for intrusion detection systems: a survey. *Appl Sci* 9(20):4396
6. Atefinia R, Ahmadi M (2021) Network intrusion detection using multi-architectural modular deep neural network. *J Supercomput* 77(4):3571–3593

7. Yadav SK, Sharma K, Kumar C et al (2022) Blockchain-based synergistic solution to current cybersecurity frameworks. *Multimed Tools Appl* 81:36623–36644. <https://doi.org/10.1007/s11042-021-11465-z>
8. Masduzzaman M, Islam A, Sadia K, Shin SY (2022) UAV-based MEC-assisted automated traffic management scheme using blockchain. *Futur Gener Comput Syst* 134:256–270
9. Weng J, Weng J, Zhang J, Li M, Zhang Y (2019) Deepchain: auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Trans Dependable Secur Comput* 18(5):2438–2455
10. Yin X, Zhu Y, Hu J (2021) A comprehensive survey of privacy-preserving federated learning: a taxonomy, review, and future directions. *ACM Comput Surv (CSUR)* 54(6):1–36
11. Berdik D, Otoum S, Schmidt N, Porter D, Jararweh Y (2021) A survey on blockchain for information systems management and security. *Inf Process Manag* 58(1):102397
12. Yadav AS, Singh N, Kushwaha DS (2023) Evolution of Blockchain and consensus mechanisms & its real-world applications. *Multimed Tools Appl* 82:34363–34408. <https://doi.org/10.1007/s11042-023-14624-6>
13. Javaid M, Haleem A, Singh RP, Khan S, Suman R (2021) Blockchain technology applications for industry 4.0: a literature-based review. *Blockchain: Res Appl* 2(4):100027
14. Moustafa N, Keshk M, Choo K-KR, Lynar T, Camtepe S, Whitty M (2021) DAD: a distributed anomaly detection system using ensemble one-class statistical learning in edge networks. *Futur Gener Comput Syst* 118:240–251
15. Li G, Dong Y, Li J, Xuekun Song (2022) Strategy for dynamic blockchain construction and transmission in novel edge computing networks. *Futur Gener Comput Syst* 130:19–32
16. Livieris IE, Pintelas E, Stavroyiannis S, Pintelas P (2020) Ensemble deep learning models for forecasting cryptocurrency time-series. *Algorithms* 13(5):121
17. Thomas C, Watson Z, Kim M, Baidya A, Lamsal M, Chowdhury MH, Basnet M, Poudel KN (2021) Cryptocurrency analysis using machine learning and deep learning. In: 2021 IEEE Signal Processing in Medicine and Biology Symposium (SPMB), IEEE, pp 01–03
18. Parekh R, Patel NP, Thakkar N, Gupta R, Tanwar S, Davidson SG, Sharma R (2022) DL-GuesS: deep learning and Sentiment Analysis-based Cryptocurrency Price Prediction. *IEEE Access* 10:35398–35409
19. Qiang W, Liu R, Jin H (2021) Defending CNN against privacy leakage in edge computing via binary neural networks. *Futur Gener Comput Syst* 125:460–470
20. Falcetta A (2022) Privacy-preserving deep learning with homomorphic encryption: an introduction. *IEEE Comput Intell Mag* 17(3):14–25
21. Cheng J, Xie L, Tang X, Xiong N, Liu B (2021) A survey of security threats and defense on Blockchain. *Multimed Tools Appl* 80:30623–30652
22. Qu Y, Yu S, Zhou W, Tian Y (2020) Gan-driven personalized spatial-temporal private data sharing in cyber-physical social systems. *IEEE Trans Netw Sci Eng* 7(4):2576–2586
23. Tramèr F, Boneh D, Paterson K (2020) Remote side-channel attacks on anonymous transactions. In: 29th USENIX Security Symposium (USENIX security 20), pp 2739–2756
24. Maji G, Mandal S, Sen S (2020) Dual image-based dictionary encoded data hiding in spatial domain. *Int J Inform Secur Priv (IJISP)* 14(2):83–101
25. Alabdulatif A, Khalil I, Yi X (2020) Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption. *J Parallel Distrib Comput* 137:192–204
26. Hu T, Liu X, Chen T, Zhang X, Huang X, Niu W, Lu J, Zhou K, Liu Y (2021) Transaction-based classification and detection approach for Ethereum smart contract. *Inf Process Manag* 58(2):102462
27. Ofori-Boateng D, Dominguez IS, Akcora C, Kantarcioglu M, Gel YR (2021) Topological anomaly detection in dynamic multilayer blockchain networks. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, Cham, pp 788–804
28. Wen H, Fang J, Wu J, Zheng Z (2021) Transaction-based hidden strategies against general phishing detection framework on ethereum, In: 2021 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, pp 1–5
29. Li S, Xu F, Wang R, Zhong S (2021) Self-supervised incremental deep graph learning for ethereum phishing scam detection. *arXiv preprint arXiv:2106.10176*
30. Qian P, Liu Z, He Q, Huang B, Tian D, Wang X (2022) Smart contract vulnerability detection technique: a survey. *arXiv preprint arXiv:2209.05872*

31. Zakzouk A, El-Sayed A, Hemdan EED (2023) A blockchain-based electronic medical records management framework in smart healthcare infrastructure. *Multimed Tools Appl* 82:35419–35437. <https://doi.org/10.1007/s11042-023-15152-z>
32. Fan H (2022) The digital asset value and currency supervision under deep learning and blockchain technology. *J Comput Appl Math* 407:114061
33. Kumar P, Kumar R, Gupta GP, Tripathi R, Srivastava G (2022) P2TIF: a Blockchain and Deep Learning Framework for privacy-preserved threat intelligence in Industrial IoT. *IEEE Trans Industr Inf* 18(9):6358–6367
34. Pan X, Zhong B, Sheng D, Yuan X, Wang Y (2022) Blockchain and deep learning technologies for construction equipment security information management. *Autom Constr* 136:104186
35. Noei M, Parvizimosaed M, Bigdeli AS, Yalpanian M (2022) A secure hybrid permissioned blockchain and deep learning platform for CT image classification. In: *2022 International Conference on Machine Vision and Image Processing (MVIP)*, IEEE, pp 1–5
36. Saveetha D, Maragatham G (2022) Design of Blockchain enabled intrusion detection model for detecting security Attacks using deep learning. *Pattern Recognit Lett* 153:24–28
37. Chancellor S, Nitzburg G, Hu A, Zampieri F, De Choudhury M (2019) Discovering alternative treatments for opioid use recovery using social media, In: *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pp 1–15
38. Zhong W, Gu F (2019) A multi-level deep learning system for malware detection. *Expert Syst Appl* 133:151–162
39. Marchetto V (2019) An investigation of cryptojacking: malware analysis and defense strategies. *J Strategic Innov Sustain* 14(1):66–80
40. Shahab S, Allam Z (2020) Reducing transaction costs of tradable permit schemes using Blockchain smart contracts. *Growth Change* 51(1):302–308
41. Yu J, Ye X, Li H (2022) A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. *Futur Gener Comput Syst* 129:399–406
42. Devi A, Kumar A, Rathee G, Saini H (2023) User authentication of industrial internet of things (IIoT) through Blockchain. *Multimed Tools Appl* 82(12):19021–19039
43. Hassan MU, Rehmani MH, Chen J (2019) Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. *Futur Gener Comput Syst* 97:512–529
44. Verma R, Dhanda N, Nagar V (2023) Application of truffle suite in a blockchain environment. In: *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*. Springer, Singapore, pp 693–702
45. Dai F, Liu G, Mo Q, Xu W, Huang B (2022) Task offloading for vehicular edge computing with edgecloud cooperation. *World Wide Web* 25(5):1999–2017
46. Mohammad Samar A, Bartoš V, Lee B (2022) GRU-based deep learning approach for network intrusion alert prediction. *Futur Gener Comput Syst* 128:235–247
47. Debicha I, Bauwens R, Debatty T, Dricot J-M, Kenaza T, Mees W (2023) TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems. *Futur Gener Comput Syst* 138:185–197

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



R. Rajmohan pursued his Doctoral Research work in Co-operative Networks under Anna University. He obtained his master's degree in Network and Internet Engineering and B.Tech. Degree in Computer Science and Engineering from Pondicherry University. He is currently working as Assistant Professor at Department of Computing Technologies, SRM Institute of Science and Technology, kattankulathur campus, Tamil Nadu, India. His fields of interest are Artificial Intelligence, Data Science, Medical Imaging, Machine Learning, Wireless Network, Deep learning and IoT. He has published numerous research works in various reputed SCI and Scopus indexed journals. He acts the associate editor of PLOS ONE journal and reviewer for reputed journals in Springer, MDPI, Tech Science Press.



T. Ananth Kumar received his Ph.D. degree in VLSI Design from Manonmaniam Sundaranar University, Tirunelveli. He received his Master's degree in VLSI Design from Anna University, Chennai and Bachelor's degree in Electronics and communication engineering from Anna University, Chennai. He is working as Assistant Professor in IFET college of Engineering affiliated to Anna University, Chennai. He has presented papers in various National and International Conferences and Journals. His fields of interest are Networks on Chips, Computer Architecture and ASIC design. He is the recipient of the Best Paper Award at INCODS 2017. He is the life member of ISTE, and few membership bodies.




S. G. Sandhya is currently pursuing her Ph.D. in the field of Machine Learning and Image Processing in the Department of Computer Science & Engineering at Annamalai University, Chidambaram, Tamil Nadu, India. She received her Master's degree in Computer Science and Engineering from Avinashilingam University for Women, Coimbatore, India, and her Bachelor's degree in Computer Software and Hardware Engineering from Avinashilingam University for Women, Coimbatore, India. She is working as Associate Professor at IFET College of Engineering, affiliated to Anna University, Chennai. She has acted as a resource person for national-level seminars. She has published many papers in various reputed journals. Her fields of interest include Machine learning, Image Processing, Data Science, Artificial Intelligence, Data Analytics, and Computer Network. She is a lifetime member of many professional bodies and acted as the editorial member for various International conferences and Symposium.



Yu-Chen Hu received his Ph.D. degree in computer science and information engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan. Currently, He is a member of Computer Vision, Graphics, and Image Processing (CVGIP), Chinese Cryptology and Information Security Association (CCISA), Computer Science and Information Management (CSIM), and Phi Tau Phi Society of the Republic of China. He joins the editorial boards of *Advances in Multimedia* (Hindawi), *Electronics* (MDPI), *IET Image Processing*, *Intelligent Automation & Soft Computing* (Tech Science Press), *Mathematical Problems in Engineering* (Hindawi), etc. His research interests include data compression, image processing, information hiding, information security, computer network, deep learning, and bioinformatics.

Authors and Affiliations

R. Rajmohan¹ · T. Ananth Kumar² · S. G. Sandhya³ · Yu-Chen Hu^{4,5} 

R. Rajmohan
rjmohan89@gmail.com

T. Ananth Kumar
tananthkumar@ifet.ac.in

S. G. Sandhya
sgsandhyadhas@gmail.com

¹ Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur Campus, Chengalpattu, Tamil Nadu, India

² Department of Computer Science and Engineering, IFET College of Engineering, Gangarampalaiyam, Tamil Nadu, India

³ Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamil Nadu, India

⁴ Department of Computer Science, Tunghai University, No. 1727, Sec. 4, Taiwan Boulevard, Xitun District, Taichung City 407224, Taiwan, Republic of China

⁵ Department of Computer Science and Information Management, Providence University, Taichung City, Taiwan, Republic of China