IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 July 2023, accepted 27 August 2023, date of publication 31 August 2023, date of current version 7 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3310576

RESEARCH ARTICLE

Ensemble Deep Learning-Based Prediction of Fraudulent Cryptocurrency Transactions

QASIM UMER[1,2], JIAN-WEI LI[3,4], MUHAMMAD REHAN ASHRAF[2], RAB NAWAZ BASHIR[2], AND HAMID GHOUS[5]

[1]Department of Computer Science, Hanyang University, Seoul 04763, South Korea
[2]Department of Computer Science, COMSATS University Islamabad, Vehari 61000, Pakistan
[3]School of Marxism, Zhejiang Gongshang University, Hangzhou 310018, China
[4]Institute of Education, Xiamen University, Xiamen 361005, China
[5]Department of Computer Science, Institute of Southern Punjab, Multan 60000, Pakistan

Corresponding author: Jian-Wei Li (jwpsy@zjsu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62177042; in part by the National Social Science Foundation, 2022 "Research on The Basic Connotation, Evaluation Criteria and Endogenous and Exogenous Cultivation Mechanism of 'Great Masters' of Ideological and Political Courses in the New Era" under Grant 22VSZ099; and in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant funded by the Korea Government [Ministry of Science and ICT (MSIT)] (Decentralized High Performance Consensus for Large-Scale Blockchains) under Grant 2021-0-00590.

ABSTRACT Cryptocurrency has emerged as a decentralized transaction to overcome the problems of the centralized transaction system. Although it has become a popular trend in online cryptocurrency transactions and mobile wallets, this method has increased the number of fraudulent transactions instead of physically transferring money. Because the shared data and the history of online transactions may lead to fraudulent transactions. The preprocess identification of fraudulent cryptocurrency transactions is becoming an urgent research question. With the exponential blossoming of Artificial Intelligence, the employing of deep learning in predicting social issues has been achieved in many disciplines. From this perspective, this paper proposes an ensemble learning approach for fraudulent cryptocurrency transactions by integrating two deep learning methods: Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM). The off-the-shelf CNN and LSTM, ensemble CNN, and ensemble LSTM with the bagged and boosted approach are compared in terms of accuracy and losses from training and test datasets. Moreover, the 10-fold cross-validation approach is employed for the evaluation of the proposed approach. The evaluation results indicate that the bagged LSTM ensembled approach is significant with 96.4% accuracy and outperforms the other approaches.

INDEX TERMS Cryptocurrency, convolutional neural networks, long short term memory, classification, blockchain.

I. INTRODUCTION

Cryptocurrency has emerged as an exciting platform with the potential to overcome problems associated with the existing modes of payments and transactions [1]. The tremendous increase in the use of cryptocurrency in the payment area has not only unlocked more opportunities and challenges but involved criminal activities [2], [3], [4]. According to one estimate, a thousand cryptocurrencies enter the market each month with different usability [5]. Moreover, more than 12000 cryptocurrencies will be available by 2022, and 70 of these cryptocurrencies have a market cap of more than one billion dollars [5]. The top ten cryptocurrencies by market cap are shown in Table 1.

Blockchains are used for the development of cryptocurrencies [6] that maintain public ledgers for managing cryptocurrency transactions [7]. Cryptocurrency transactions are decentralized and recorded in a peer-to-peer network called a blockchain [8], [9], eliminating the need for a central authority [10]. Bitcoin is a pioneering cryptocurrency, but there are also many other coins with significant potential. For example, Ethereum is the second-largest cryptocurrency

The associate editor coordinating the review of this manuscript and approving it for publication was Nazar Zaki.

TABLE 1. Market cap of top five cryptocurrencies [13].

Cryptocurrency	Market Cap
Bitcoin (BTC)	$415,203,289,281
Ethereum (ETH)	$148,730,510,731
Tether (USDT)	$65,953,462,664
USD Coin (USDC)	$55,557,354,390
Binance Coin (BNB)	$39,260,543,387

FIGURE 1. An overview of Ethereum's value [5].

by market capitalization [6] that allows smart contracts [11]. An overview of Ethereum's value is presented in Fig. 1. The Bitcoin network has a limited capacity to handle many transactions quickly; therefore, it is not scalable [10]. Ethereum reduces the problem of the scalability of Bitcoin [10]. Vitalik Buterin develops Ethereum to delegate power to the user [10]. The main advantage of Ethereum is its low transaction fee (gas) [12] required to execute a transaction on Ethereum, regardless of transaction success or failure. Each gwei (Ethereum gas unit) is equal to 0.000000001 ETH (10^{-9} ETH). Ethereum is more adaptable to smart contracts and transactions [1]. Smart contracts are a type of Ethereum account. This means they have a balance and can be the target of transactions. Therefore, fraudulent transactions may occur through smart contracts.

The decentralized blockchain approach allows operations without central control and intermediaries with several benefits related to privacy and security [14], e.g., transaction anonymity [15]. Such benefits make fraudulent behavior very common [16], i.e., the decentralized control of blockchain and transactions' anonymity leads to frequent fraudulent transaction behavior in cryptocurrency [17], [18]. According to CipherTrace, a cryptocurrency forensics company's scam led to a loss of 4.5 billion dollars in 2019. Moreover, the cryptocurrency monitoring companies declared that Ethereum is the foremost choice for fraudulent transactions [6]. Although a user's anonymity is very suitable for fraudulent transactions with any Cryptocurrency network [19], [20], the lack of control by an authority and anonymity is very attractive for fraudulent activity [21].

The Ponzi scheme is one of the most vibrant scams associated with cryptocurrency. The masquerading schemes are common on the Ethereum network [22]. Because of immutability and user anonymity, fraudulent transactions are difficult to reverse, thus making them very attractive for fraudulent transactions [23]. It is also very difficult and time-consuming to manually sort for fraudulent transactions. Such a huge set of transactions makes detecting fraudulent transactions nearly impossible. The problem is also hard regarding time and other resources required to detect abnormal activities [23]. Machine learning is an ideal candidate for this purpose. Many efforts were put into effect using machine learning to detect anomalous activity from a different perspective [16], [22], [24], [25], [26].

The purpose of the proposed solutions is to detect fraudulent transactions using a machine learning model. The study aims to detect fraudulent transactions on the Ethereum platform with limited features. Note that we select the Ethereum platform because it is widely acceptable and more adaptable to smart contracts. Machine learning approaches are widely applied to improve the accuracy of identifying fraudulent transactions. Out of these approaches, Artificial Neural Network (ANN)-based approaches [27] are more accurate. The study wants to improve the accuracy of detecting fraudulent transactions in Ethereum using ensemble deep learning approaches. The study also aims to explore the performance of different ensemble models to detect the occurrence of fraudulent transactions using ensemble deep learning models.

The paper highlights are as follows:

- Identification of the fraudulent transactions on the Ethereum network with high accuracy.
- Introduction of an ensemble machine learning approach to improve the accuracy of identification of fraudulent transactions on the Ethereum network.
- In-depth comparison of different machine learning models against the proposed ensemble approach of identification of fraudulent transactions.

The rest of the paper is organized as follows. A literature review is given in Section II. The material and method are given in Section III. Section IV is for results and discussion. Finally, the concluding remarks and future work is discussed at the end.

II. RELATED WORK

Sun Yin et al. [28] proposed supervised machine learning-based anomaly and criminal activity detection in a Bitcoin-based ecosystem. The proposed solution is based on a dataset of 395 million transactions with 957 unique clusters. The study also compares the performance of Random Forests (RF), Decision Trees (DT), K-Nearest Neighbour (KNN), Gradient Boosting, Ada Boosting and Bagging classifiers for performance detection of anomalies in Bitcoin-based systems. The Gradient Boosting is the most accurate out of the seven tested models, with 80.83% accuracy.

Many researchers [1], [2], [3], [4], [29] proposed machine learning-based detection of abnormal activity detection in the Ethereum network. The study also compares the performance of Naïve Bayes (NB), Multilayer Perception (MLP), Support Vector Machine (SVM), RF, and KNN. The SVM and RF

are the most accurate out of the tested models, with 99.66% accuracy in predicting the abnormal activity detection in Ethereum.

Wu et al. [30] and Kumar et al. [31] proposed machine learning-based abnormal activity detection from suspicious users in Ethereum platforms. The study also compares the performance of the different machine-learning algorithms. Among them, DT and RF are the most significant with accuracies of 83.66% and 98.93%, respectively.

Hu et al. [32] proposed LSTM based machine-learning approach for detecting anomalies in smart contracts in the Ethereum network. The proposed solution shows high precision in identifying anomalies in smart contracts in the Ethereum network. Tan et al. [25] proposed a graph Convolution Neural Network (CNN) to identify ambiguous transactions with 95% accuracy.

Yuan et al. [33] proposed machine learning-based phishing detection on the Ethereum network. The proposed solution detects fraudulent transactions by transaction information with 84.6% accuracy. Ibrahim et al. [34] proposed an ensemble machine learning model with high accuracy using the SVM and RF-based models. Tsaur et al. [35] proposed account attributes and opcode functionality with XGBoost to 95% precision to detect illicit transactions.

Chen et al. [36] proposed a solution to identify the Ponzi scheme on the Ethereum network using a supervised machine learning approach. The RF-based approach can identify 305 out of 394 Ponzi schemes from the test dataset with more than 90% probabilistic confidence. Singh et al. [4] proposed the temporal debiasing method by using Graph Neural Network (GNN) approach for fraud detection in cryptocurrency. The study compared the performance of different machine learning models and benchmarked the performance of the proposed solution with existing models.

Lee and Wei [37] proposed an exploratory simulation model to detect the anomaly in the Bitcoin system. The proposed simulation model helps to reduce double-spending risks with absolute accuracy. Monamo et al. [38] recommended Unsupervised Anomaly Detection, which finds outliers in trends using trimmed k-means. This portion is compared with the dataset of known fraud. Experimental results show that the proposed approach achieves precision performance on benchmark datasets.

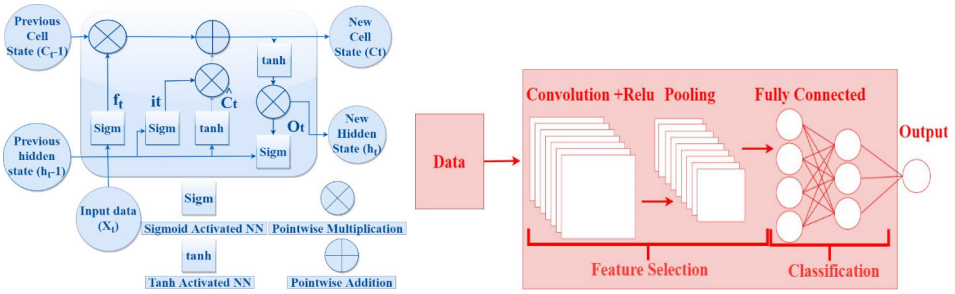
Sayadi et al. [39] proposed a solution to detect fraudulent transactions in cryptocurrency and proposed a technique to determine anomalies in electronic transactions of Bitcoin by machine learning, with high accuracy with k-mean and SVM. Chen et al. [40] proposed machine learning-assisted solutions to detect Bitcoin theft transactions. The performance of five machine learning models (KNN, SVM, RF, AdaBoost, and MLP) is evaluated to identify the theft transactions in Bitcoin. The study results reveal that the RF performs best, with an F1-value of 95.9%. Kasera [41] proposed an artificial intelligence-based approach for identifying fraud in cryptocurrency. This study focuses on how artificial intelligence provides us with an empirical framework to identify such frauds to ensure more security in the crypto-sphere.

Digital currency has become more popular in this era. According to this research, some critical issues of anomalous behavior are also associated with it that cause serious problems for cryptocurrencies. Arya et al. [42] proposed ML techniques to detect the anomalous behavior of the crypto-currency by using the Bitcoin dataset. The proposed solution is based on the multivariate Gaussian distribution, 2-phase clustering, and one-class SVM algorithms to detect the outliers in the Bitcoin dataset. It is identified from the results that the multivariate Gaussian distribution algorithm has more accuracy as compared to the other models.

Pham and Lee [43] focused on detecting the anomaly, especially in the Bitcoin transaction. The study's main aim is to identify suspicious transactions and user behavior. The study used k-means, unsupervised SVM, and clustering machine learning techniques. Zarpelão et al. [15] proposed a command and control approach based approach on the network of Bitcoin. In this case, the group of transactions is made based on the users. In the next step, features of every transaction's group are identified to detect their behavior, such as whether they act systematically or not. An algorithm named ''OSVM'' was proposed for this analysis to obtain samples from users with legal behavior only. In this case, the ZombierCoin botnet and Bitcoin blockchain are used to conduct the test in a closed environment. According to the depicted results, the proposed technique is more useful in detecting the bots having a low rate of FP (false positive) in the different cases.

Farrugia et al. [44] mainly focused on identifying illicit IDs on the blockchain of the Ethereum coin. The proposed three machine learning models named DT, RF, and KNN are used to detect fraud on the Ethereum blockchain. The study shows significant improvement in time measurement with the help of machine learning techniques.

Although the above-discussed studies propose machine/deep learning-based approaches (i.e., DT [45], RF [46], SVM [47], and ANN [27]) to identify the different types of abnormalities and anomalies in different types of cryptocurrency platforms, performance improvement is required to avoid anomalies in cryptocurrency transactions. In this perspective, this paper proposes an ensemble machine learning model with CNN and LSTM to improve accuracy in identifying fraudulent transactions, which is different and effective in contrast to off-the-shelf CNN and off-the-shelf LSTM models. Notably, Off-the-shelf CNN and off-the-shelf LSTM refer to pre-trained CNN that are readily available and can be used for various tasks without the need for extensive training from scratch. We combined LSTM and CNN for the ensemble approach because of their specific strengths in processing sequential and structural data, respectively. Fraudulent cryptocurrency transactions often exhibit patterns that can be captured through sequential analysis. However, cryptocurrency transaction data can have a structural aspect, i.e., the relationships between entities. By combining LSTM and



(a) Off-the-shelf LSTM Architecture (b) Off-the-shelf CNN Architecture

FIGURE 2. Off-the-shelf CNN and LSTM architectures.

CNN, LSTM can capture temporal patterns and dependencies within individual transactions or sequences of transactions, while CNN can extract structural features from the transaction data.

III. METHODOLOGY

The objective of the study is to find a function that can determine the occurrence of fraudulent transactions y from a set X of features by Eq. 1.

$$F(X) \rightarrow y \tag{1}$$

where, X is the set of features with inputs given in Eq. 2.

$$X = x_1, x_2, \ldots, x_n \tag{2}$$

The set of features X is used to predict the occurrence of fraudulent transaction y. The study uses LSTM and CNN with an ensemble approach for predicting the occurrence of fraudulent transactions.

A. OFF-THE-SHELF LSTM

The Long Short Term Memory (LSTM) architecture is shown in Figure 2a. Recurrent Neural Network (RNN) is a deep learning technique that can retain information from previous input that is impossible with shallow ANN. In RNN, the states of the input layer change with each input; therefore, the RNN suffers from long-term memory. LSTM is an extension of the Recurrent Neural Network (RNN) that overcomes the problem of long-term memory. LSTM is an RNN-type model that can manage the long-term memory to manage the long terms trends in data. For this purpose, the LSTM uses the memory cells whose state management operations are managed by the gates. The ability to retain long-term context is useful for problems that require previous contextual data in predictions. The new input data and previous hidden states are fed into the model. The model generates the vectors of the element with values in the range of 0 and 1 with the sigmoid function. The model is trained so that the forget gate is close to 1 when the output is relevant and 0 when the output is irrelevant. Moreover, LSTM can maintain long-term memory with memory cells and gates instead of a hidden layer. The additional state $S_{o_{ti}}$ at time instant t_i is maintained by the output of the forget gate is mentioned by f_t by Eq. 3, where t is the timestamp, x_t is the input, h_{t-1} is the previous hidden state, W_i is the weighted matrix, and b_t is the bias. Forget gate f_c decides which information must retain and which to ignore.

$$f_t = \sigma(W_i.[h_{t-1}, x_t] + b_t) \tag{3}$$

The information from current input x_t and hidden state h_{t-1} are passed through the sigmoid function that produces values between 0-1. The value of f_t is used for point-to-point multiplication.

The input gate i_t is used to update the cell status. The previous hidden state h_{t-1} and current state x_t are passed through another sigmoid function to classify inputs into important (1) and non-important (0). The i_t function is expressed by Eq. 4, where t is the time stamp, i_t is the input gate, W_r is the weight matrix, and b_f is the bias vector. Moreover, $\tilde{C}_t$ is the value by tan_h function expressed by Eq. 5, where W_c is the weighted matrix of tan_h, b_c is the bias vector concerning W_c.

$$i_t = \sigma(W_r.[h_{t-1}, x_t] + b_f) \tag{4}$$

$$\tilde{C}_t = tan_h(W_c.[h_{t-1}, x_t] + b_c) \tag{5}$$

The forget vector f_t is multiplied by the previous cell state C_{t-1}. The output of this operation is the point-to-point addition with the output of input vector i_t to produce a new cell state C_t expressed by Eq. 6.

$$C_t = f_t \times C_{t-1+i_t} \times \tilde{C}_t \tag{6}$$

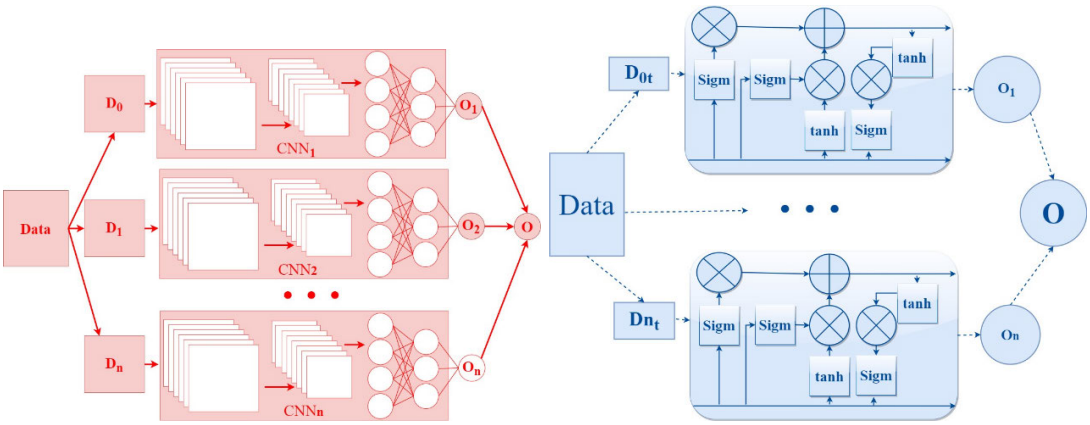
The output gate O_t is used to determine the next hidden state by the current state and previous hidden state h_{t-1} through the sigmoid function expressed by Eq. 7. The hidden state h_t is used for making predictions expressed by Eq. 8.

$$O_t = \sigma(W_o.[h_{t-1}, x_t] + b_o) \tag{7}$$

$$h_t = O_t \times tan_h \tilde{C}_t \tag{8}$$

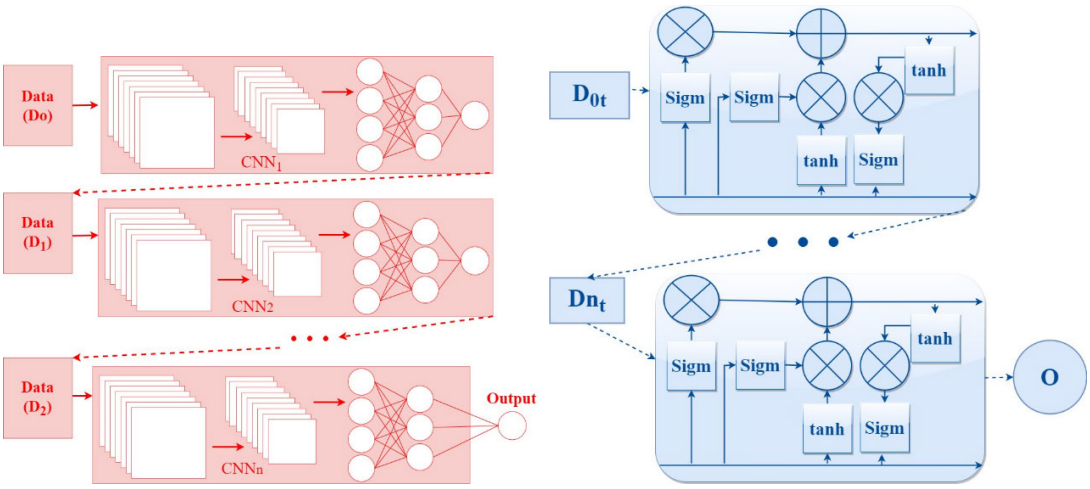
B. OFF-THE-SHELF CNN

Although CNN is commonly used for computer vision-based solutions, it is also achieved promising results in other domains. CNN is based on various layers where the output of each layer is connected to regions of input features. This operation involves convolving the input features to model



(a) Bagged CNN Architecture (b) Bagged LSTM Architecture

FIGURE 3. Bagged CNN and LSTM architectures.



(a) Boosted CNN Architecture (b) Boosted LSTM Architecture

FIGURE 4. Boosted CNN and LSTM architectures.

filters for pattern recognition in the input data. The convolution layer is the first type of layer in the CNN architecture, as shown in Figure 2b.

Each convolution layer is defined by Eq.9, Eq. 10, and Eq. 11, where ϕ is the filter at layer 1 (M_n), Φ is the filter at layer 2 (L_n), and ω is the filter at layer 3 (G_n).

$$M_n = f(I_n; \phi_1, \phi_2, \ldots, \phi_k) \tag{9}$$

$$L_n = f(M_n; \Phi_1, \Phi_2, \ldots, \Phi_k) \tag{10}$$

$$G_n = f(M_n; \omega_1, \omega_2, \ldots, \omega_k) \tag{11}$$

Note that we select CNN over ANN (the most significant state-of-the-art approach) because CNN tends to be a more powerful and accurate way of solving classification problems and high accuracy in weight sharing [48].

C. ENSEMBLE MODELS

Ensemble machine learning models [49] are the techniques to combine multiple models for predicting optimal results by combining their output. An ensemble machine learning multiple models are used rather than a single model to improve accuracy and consistency. Using multiple machine learning rather than a single model can produce optimal models. Bagging and boosting [50] are the most common techniques of ensemble machine learning models. Both techniques are applied using CNN and LSTM models. Using the bagging and bootstrap aggregating, four architectures (bagged CNN, Bagged LSTM, Boosted CNN, and Boosted LSTM) of ensemble machine learning models are made to predict fraudulent transactions on the Ethereum platform.

In the case of the bagging technique, multiple models are trained in parallel on a subset of the dataset. The output of each model is combined to produce a single output. The architecture of bagging CNN and bagged LSTM is shown in Figure 3 where Figure 3a presents the bagged CNN architecture and Figure 3b presents the bagged LSTM architecture. The dataset is partitioned into a subset for multiple models

Algorithm 1 Bagged CNN and Bagged LSTM

procedure Bagged CNN and Bagged LSTM
  Input: X, y, N^g
  Initialize: $h \leftarrow 1$
  while $h \leq N^g$ **do**
    $(X_h, y_h) \leftarrow \int rep(X, y)$ // generate subset (X_h, y_h) of (X, y) for random sampling with a replacement function $\int rep$
    $X_h \xrightarrow{\int_h^g(\sigma, W_h^g, b_h^g)} y_h$ // Training of the h^{th} model in an ensemble using the (X_h, y_h)
    $h \leftarrow h + 1$
  end while
  Output: $\int_1^g(\sigma, W_1^g, b_1^g), \ldots, \int_N^g(\sigma, W_{N_g^g}, b_{N_g^g})$
end procedure

where, X is the set of features extracted from correlation analysis mentioned in Section III-E, y is the instance of the occurrence of a fraudulent transaction, N^g is the total number of the model in bagging, h is the current model, X_h is the subset of feature set X for h model, y_h is the instance of fraudulent transaction for h model, $\int rep$ is the replacement function, σ is the non-linear activation function, W is the weights, b is the bias, and $\int_1^g(\sigma, W_1^g, b_1^g), \ldots, \int_N^g(\sigma, W_{N_g^g}, b_{N_g^g})$ are the set of models (CNN and LSTM) in bagging.

Algorithm 2 Boosted CNN and Boosted LSTM

procedure Boosted CNN and Boosted LSTM
  Input: X, y, N^b, α^t
  Initialize: $h \leftarrow 2$
  $X \xrightarrow{\int_1^b(\sigma, W_1^b, b_1^b)} y$ // Train Initial model (X,y)
  while $h \leq N^b$ **do**
    $t_{temp} \leftarrow y - \alpha^b \sum_{m=1}^{h=1} \int_m^b(.)$
    $X \xrightarrow{\int_h^b(\sigma, W_h^b, b_h^b)} y_{temp}$ // Train Initial model (X,y)
    $h = h + 1$
  end while
  Output: $\int_1^b(\sigma, W_1^b, b_1^b), \ldots, \int_N^b(\sigma, W_{N_{bg}^b}, b_{N_{bg}^b})$
end procedure

where, X is the set of features extracted from correlation analysis mentioned in Section III-E, y is the instance of the occurrence of a fraudulent transaction, N^b is the total number of the models in boosting, α^t are weights in boosting models, h is the current model, α is nonlinear activation, W is the weights, b is the bias, $\int_1^b(\sigma, W_1^b, b_1^b)$ is the h^{th} model, and $\int_1^b(\sigma, W_1^b, b_1^b), \ldots, \int_N^b(\sigma, W_{N_{bg}^b}, b_{N_{bg}^b})$ are the set of models (CNN and LSTM) in boosting.

in both architectures, and the output is combined to produce optimal results. The results of each model are combined as expressed in Eq. 12.

$$\int_1^g(\sigma, W_1^g, b_1^g), \int_2^g(\sigma, W_2^g, b_2^g), \ldots, \int_N^g(\sigma, W_{N_g^g}, b_{N_g^g}) \tag{12}$$

Algorithm 3 Integrated Ensemble Model

procedure Integrated Ensembled Model
  Input: $X_{t_{T+1}}$, $\alpha_{\frac{g}{b}}$, $\int_h^{\frac{g}{b}}(\sigma, W_h^{\frac{g}{b}}, b_h^{\frac{g}{b}}) \cdots \int_{N_{\frac{g}{b}}^{\frac{g}{b}}}^{\frac{g}{b}}(\sigma, W_{N_{\frac{g}{b}}^{\frac{g}{b}}}^{\frac{g}{b}}, b_{N_{\frac{g}{b}}^{\frac{g}{b}}}^{\frac{g}{b}})$
  Initialize: $\hat{y}_{t+1}, h \leftarrow 2$
  $X \xrightarrow{\int_1^t(\sigma, W_1^t, b_1^t)} y$
  while $h \leq N^{\frac{g}{b}}$ **do**
    $\hat{y}_{t_{T+1}} \leftarrow \hat{y}_{t_{T+1}} + \alpha^{\frac{g}{b}} \int_h^{\frac{g}{b}}(\sigma, W_b^{\frac{g}{b}}, b_h^{\frac{g}{b}}, X_{t_{T+1}})$
    $h = h + 1$
  end while
  Output: $\hat{y}_{t_{T+1}}$
end procedure

where, $X_{t_{T+1}}$ is the feature set at time instances, $\alpha_{\frac{g}{b}}$ are Weights of bagging or boosting, $\int_h^{\frac{g}{b}}(\sigma, W_h^{\frac{g}{b}}, b_h^{\frac{g}{b}}) \cdots \int_{N_{\frac{g}{b}}^{\frac{g}{b}}}^{\frac{g}{b}}(\sigma, W_{N_{\frac{g}{b}}^{\frac{g}{b}}}^{\frac{g}{b}}, b_{N_{\frac{g}{b}}^{\frac{g}{b}}}^{\frac{g}{b}})$ are set of ensembled bagged or boosted models, $\hat{y}_{t_{T+1}}$ is the output of the ensembled model, X is the feature set, Y is the instance of the output, α is the activation function, and $W_b^{\frac{g}{b}}$ are Weights of bagging or boosting models.

The algorithms for bagged CNN and bagged LSTM are given by algorithm 1.

In the case of boosting CNN and boosting LSTM, the multiple models are trained in sequence, and the base model depends upon the previous model's output. The architecture of boosted CNN and boosted LSTM is shown in Figure 4 where Figure 4a presents the boosted CNN architecture and Figure 4b presents the boosted LSTM architecture.

The algorithms for boosted CNN and boosted LSTM are given by algorithm 2.

The predictions by bagged CNN, bagged LSTM, boosted CNN, and boosted LSTM is made by algorithm 3.

D. CONFIGURATION OF MODELS

The configuration details of the model are given in Table 2. A similar configuration is used for individual and ensemble approaches for each layer. These parameters are optimum with the best accuracy. The maximum accuracy is achieved with 300 epochs, and accuracy above 300 is unaffected. Note that we have tried the off-the-shelf algorithms with multiple parameter tuning. However, none of them contributed to performance improvement. Therefore, we selected ensemble approaches.

E. DATASET

We collected the public dataset from Kaggle [51] and reused it for detecting fraudulent transactions in Ethereum. Note that we select the Ethereum platform because it is widely acceptable and more adaptable to smart contracts. Second, datasets about the fraudulent transaction of other cryptocurrencies are not publicly available. We performed the correlation

TABLE 2. Configurations.

Parameter	CNN	LSTM
No hidden layers	2	2
Activation Function at the input layer	Relu	Relu
Activation Function at hidden layer 1	Relu	Relu
Activation Function at hidden layer 2	Relu	Relu
Activation Function at the output layer	Sigmoid	Sigmoid
Optimizer	Adam	Adam
No of Epochs	300	300
Training test ratio	80:20	80:20
No Nodes at input layer	46	46
No Nodes at hidden layer 1	46	46
No Nodes at hidden layer 2	30	30
No Nodes at output layer	1	1

analysis for the identification of important features by dropping the highly correlated feature (> 0.8) to escape the curse of dimensionality. The Pearson correlation method is used for the correlation analysis where the minimum number of observations is 1. The correlations between features and the occurrence of fraudulent and non-fraudulent transactions are shown in Figure 5a and Figure 5b, respectively. The dark and light colors of the chart depict the strong and weak relationship between features and the occurrence of fraudulent and non-fraudulent transactions. Notably, the exploited dataset is imbalanced [51]. Therefore, we perform re-sampling to correct the bias in the original dataset. We only consider the under-sampling for our experiments by randomly selecting the n samples from the majority class, where n is the number of samples from the minority class. We avoid over-sampling because it involves replicating minority class samples to increase their representation in the dataset and can lead to overfitting [52], where the model becomes overly specialized to the minority class and performs poorly on unseen data. Moreover, it may artificially improve performance metrics [53], i.e., accuracy.

IV. EVALUATIONS

The performance of selected models is compared using the accuracy and loss from the training and test dataset. The dataset is partitioned into a 80:20 ratio for the training and testing against each fold. The training and test accuracy of each model is analyzed and compared.

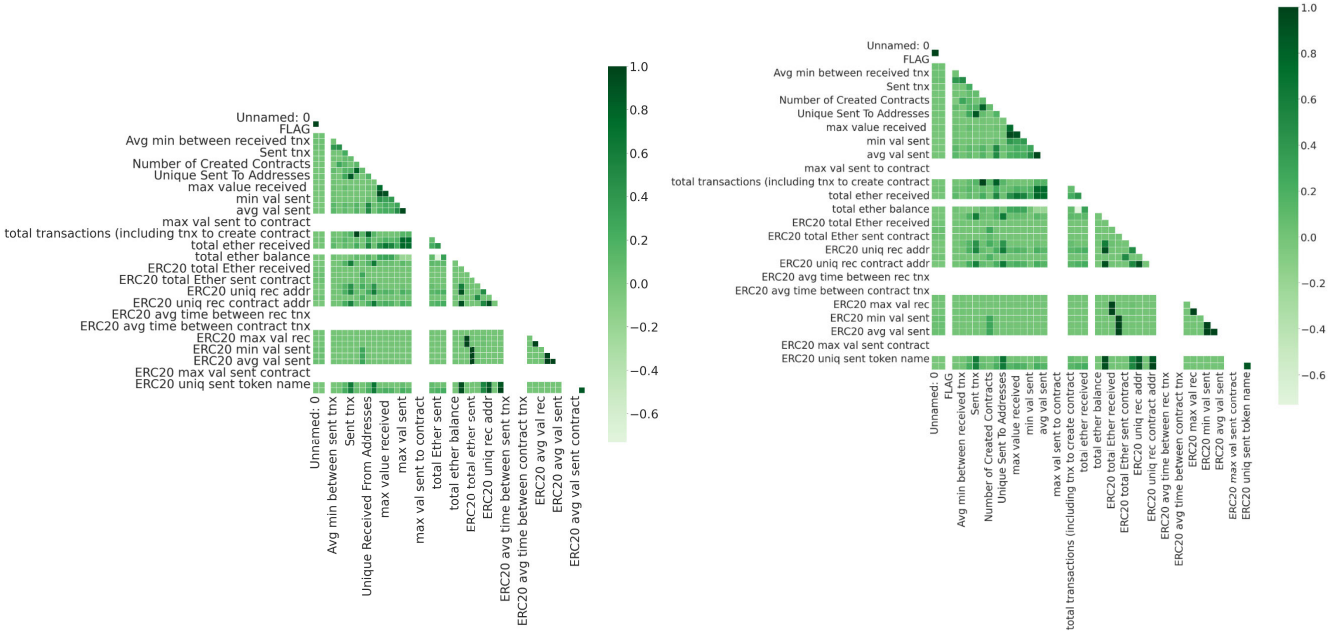
Accuracy is the measure of correct predictions out of total predictions l expressed by Eq. 13. The accuracy of each model is observed over three hundred epochs.

$$Accuracy = \frac{Correctpredictions}{Totalpredictions} \tag{13}$$

The 10-fold cross-validation results of six approaches are presented in Figure 6, and the following observations are made:

- The training and testing accuracy for detecting fraudulent transactions by bagged LSTM model is 96% and 96.4% with training and test datasets. Figure 6 presents the accuracy of LSTM and CNN with bagged, boosted, and simple LSTM/CNN. The accuracy of the model from training and testing datasets over 300 epochs is displayed in Figure 6a. Figure 6a shows that the bagged LSTM model is in a balanced shape. Consequently, the bagged LSTM ensemble model is more accurate than other tested models.
- The training and testing accuracy (shown in Figure 6b) for detecting fraudulent transactions by boosted LSTM model is 95% and 94.5%, respectively. The boosted LSTM model is also in a balanced shape. The accuracy of the boosted LSTM over 300 epochs is shown in Figure 6c for both the training and testing datasets, respectively. The accuracy of the boosted LSTM is less than the bagged LSTM for both the training and test datasets.
- The accuracy of off-the-shelf LSTM for both the training and testing dataset is shown in Figure 6c. The individual LSTM is also in optimum shape. The training and testing accuracy of individual LSTM reaches a maximum of 94.7% and 90.5% over 300 epochs, respectively. The training and test accuracy of individual LSTM is less than the bagged LSTM and boosted LSTM.
- The training and testing accuracy for detecting fraudulent transactions by the bagged CNN model is 95% and 94%, respectively. The accuracy of bagged CNN over 300 epochs is shown in Figure 6d. The bagged CNN model is also balanced to make predictions for detecting fraudulent transactions over time. The accuracy of the bagged CNN is less than the bagged LSTM, boosted LSTM, and off-the-shelf LSTM models from both training and test datasets.
- The accuracy of boosted CNN for training and testing datasets over 300 epochs is shown in Figure 6e. The boosted CNN model is also optimum fitted to predict the occurrence of fraudulent transactions over time. The maximum accuracy of boosted CNN from training and testing datasets is 89% and 86%, respectively. The accuracy of boosted CNN is less than the bagged CNN, bagged LSTM, boosted LSTM, and off-the-shelf LSTM.
- The accuracy of individual CNN over 300 epochs for training and testing datasets is shown in Figure 6f. The maximum accuracy of the CNN model is 85.7% and 85.6%, respectively. The accuracy of the off-the-shelf CNN is less than all selected models for detecting fraudulent transactions in Ethereum-based cryptocurrency transactions.

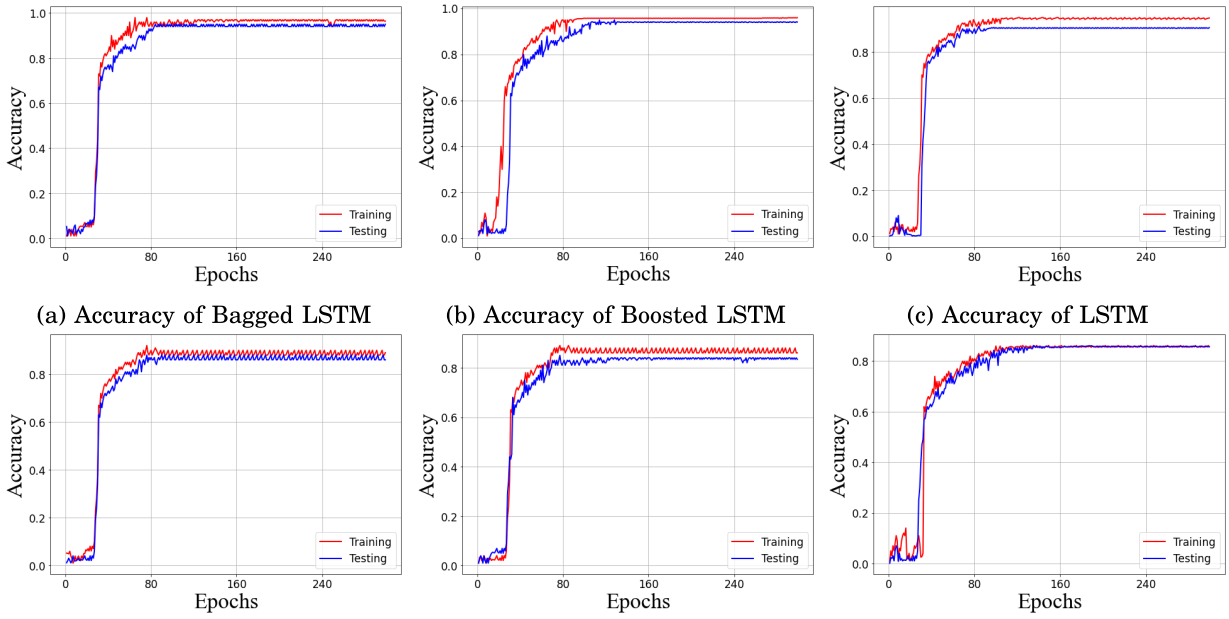
Moreover, Figure 7 presents the comparison of training and testing accuracy of all the selected models and The



(a) Correlation between features and the occurrence of fraudulent transactions

(b) Correlation between features and the occurrence of non-fraudulent transactions

FIGURE 5. Correlation between features and the occurrence of fraudulent and non-fraudulent transactions.



(a) Accuracy of Bagged LSTM

(b) Accuracy of Boosted LSTM

(c) Accuracy of LSTM

(d) Accuracy of Bagged CNN

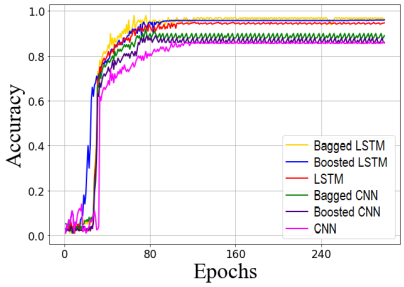
(e) Accuracy of Boosted CNN

(f) Accuracy of CNN

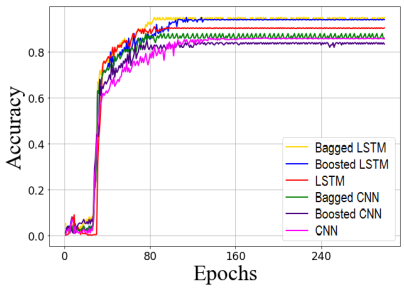
FIGURE 6. Accuracy with bagged, boosted, and off-the-shelf LSTM/CNN.

maximum accuracy achieved by each model, respectively. From Figure 7, the following observations are made:

- The accuracy of the training dataset of each selected model is shown in Figure 7a for comparison purposes. From Figure 7a, it is clear that the bagged LSTM offers high accuracy as compared to other selected models. The accuracy of CNN is less than all of the selected models. It is also important to observe that the accuracy of LSTM is more than the bagged CNN and boosted CNN. The accuracy of each model from the testing dataset is shown in Figure 7b for comparison purposes. The bagged LSTM is more accurate than other models with



(a) Comparison of training accuracy of selected models



(b) Comparison of testing accuracy of selected models

FIGURE 7. Comparison of training/testing accuracy of selected models.

the testing dataset. The performance of the LSTM in terms of accuracy is better than the ensemble CNN and individual CNN for detecting fraudulent transactions in Ethereum-based transactions.

- The maximum accuracy for detecting fraudulent transactions is achieved through the bagged LSTM model. The accuracy of the bagged LSTM model is 96% through the training dataset and 96.4% through the testing dataset. The CNN model is the least accurate compared to other models, with the training and testing dataset, with 85.7% and 85.7% accuracy, respectively. Note that bagging decreases variance, not bias, and solves over-fitting issues in a model. Therefore, the proposed model significantly improves the performance of the classifier.

Finally, the loss measures the difference between the predicted and actual values expressed by Eq. 14. Loss is the measure of the difference between predicted and actual values. Although the loss is the inverse function of accuracy, it helps the researchers/readers better understand the evaluation results. Therefore, we compute the losses of the selected models in this paper.

$$Loss = abs(PredictedValue - ActualValue) \tag{14}$$

It is a binary classification problem to detect the occurrence of a fraudulent transaction or not. The loss for the problem is measured in the form of binary cross-entropy, also named log loss. The binary cross-entropy is the negative average of the log of corrected predicted probabilities expressed by Eq. 15.

$$LogLoss = \frac{1}{N}\sum_{i=0}^{N} -(y_i \times log(pi) + (1 - y_i) \times log(1 - pi)) \tag{15}$$

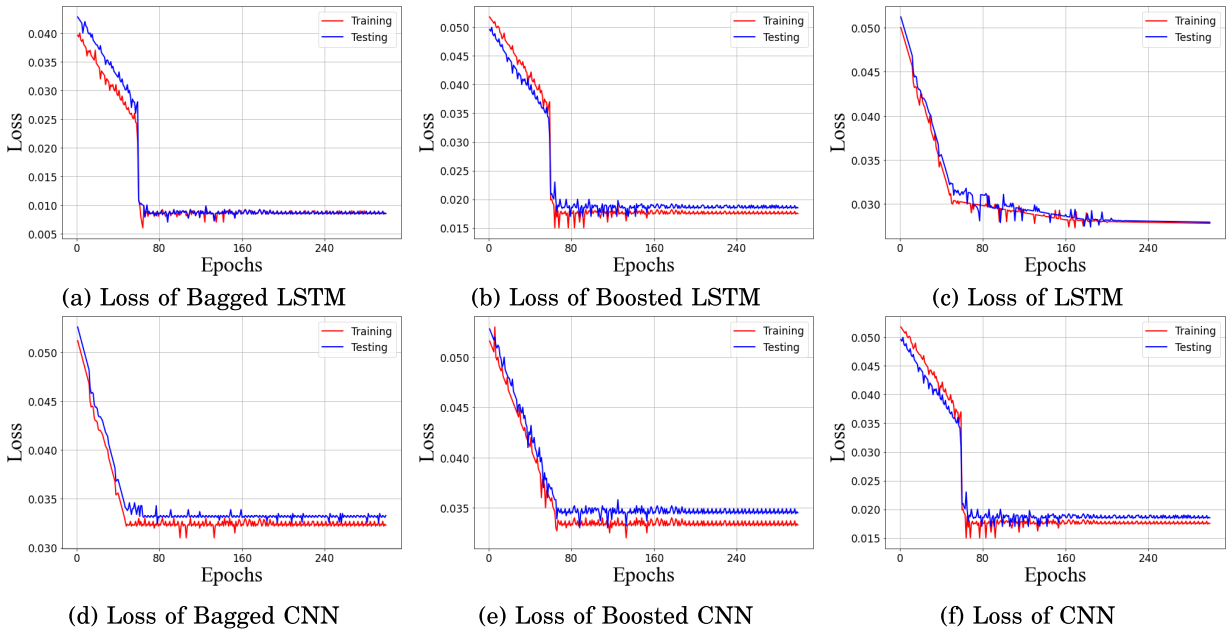
where, pi is the probability of the occurrence of a fraudulent transaction and (1)-pi) is the probability of the occurrence of non-fraudulent transactions. The log loss of selected models is analyzed against the training and test datasets.

Figure 8 presents the losses of LSTM and CNN with bagged, boosted, and simple LSTM/CNN. The log losses of bagged LSTM for training and testing datasets over three hundred epochs are shown in Figure 8a. The minimum log losses with the training and testing dataset are 0.0273 and 0.0274, respectively. The loss with the bagged LSTM ensemble model is less than the other tested models. The log losses of boosted LSTM for training and testing datasets over three hundred epoch is shown in Figure 8b. The minimum log losses with the training and testing dataset are 0.017 and 0.017, respectively. The log losses of individual LSTM for training and testing datasets over three hundred epochs are shown in Figure 8c. The minimum log losses with the training and testing dataset are 0.0273 and 0.0274, respectively.

The log losses of bagged CNN for training and testing datasets over three hundred epoch is shown in Figure 8d. The minimum log losses with the training and testing dataset are 0.031 and 0.00325, respectively. The log losses of boosted CNN for training and testing datasets over three hundred epochs are shown in Figure 8e. The minimum log losses with the training and testing dataset are 0.032 and 0.033, respectively. The log losses of individual CNN for training and testing datasets over three hundred epoch is shown in Figure 8f. The minimum log losses with the training and testing dataset are 0.0421 and 0.043, respectively. The individual CNN is least efficient in reducing the losses with training and test datasets compared to others selected models for comparison purposes.

Figure 9 compares all the selected models' training and testing losses. The losses of each model with the training and testing dataset are shown in Figure 9a and Figure 9b, respectively. It can be observed that the bagged LSTM ensemble model is more efficient in reducing losses than the other models. The off-the-shelf CNN model is less efficient in reducing losses than the other models. The bagged LSTM ensemble model is more efficient in reducing losses than the other model.

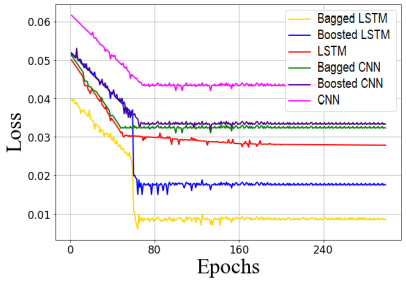
The bagged LSTM model is more accurate compared to the selected models. The state-of-the-art approach for detecting fraudulent transactions achieved an accuracy of 94% [6]. The proposed ensemble learning model achieved an accuracy of 96.4%. The proposed ensemble LSTM model is also more efficient in reducing error than the state-of-the-art approach.



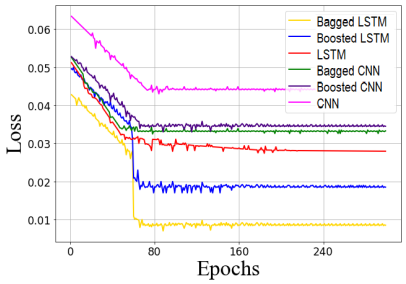
(a) Loss of Bagged LSTM (b) Loss of Boosted LSTM (c) Loss of LSTM

(d) Loss of Bagged CNN (e) Loss of Boosted CNN (f) Loss of CNN

FIGURE 8. Losses with bagged, boosted, and simple LSTM/CNN.



(a) Comparison of training log loss of selected models



(b) Comparison of testing log loss of selected models

FIGURE 9. Comparison of training/testing log losses of selected models.

A. THREATS TO VALIDITY

The implementation of the proposed approach gives rise to concerns about internal validity. To ensure its accuracy, we perform cross-checks; however, it is possible that some errors may have been unintentionally overlooked.

The generalization of the proposed approach is a matter of concern in terms of external validity. Our analysis focuses exclusively on fraudulent transactions involving Ethereum, and the performance of the approach may differ when applied to the prediction of fraudulent transactions in other cryptocurrencies.

Additionally, the limited number of fraudulent transactions poses a threat to external validity. Deep learning algorithms typically require fine-tuning parameters and a substantial amount of training data to achieve optimal performance. The scarcity of fraudulent transactions may restrict the applicability of our results and hinder a comprehensive exploration of the parameter space.

V. CONCLUSION

The study proposed ensemble deep machine learning models to predict the occurrence of fraudulent transactions in the Ethereum network to improve the predicting accuracy of fraudulent transactions. For this purpose, off-the-shelf CNN, off-the-shelf LSTM, and ensemble approaches are tested and compared for performance. For ensemble deep learning, the bagged and boosted approach is used. Out of the six models (off-the-shelf CNN, off-the-shelf LSTM, bagged CNN, bagged LSTM, boosted CNN, and boosted LSTM), the bagged LSTM is more accurate compared to other models evaluated for the comparison approach. Moreover, the bagged LSTM approach is 2.4% more accurate than the state-of-the-art approach for detecting fraudulent transactions in Ethereum. In future, we would like to investigate the practical applications of the proposed approach by implementing it in blockchain technology using smart contracts.

REFERENCES

[1] M. J. Shayegan and H. R. Sabor, "A collective anomaly detection method over Bitcoin network," 2021, *arXiv:2107.00925*.

[2] B. Podgorelec, M. Turkanović, and S. Karakatič, "A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection," *Sensors*, vol. 20, no. 1, p. 147, Dec. 2019.

[3] P. K. Choudhary, "Fraudulent account recognition using supervised learning in Ethereum," Ph.D. dissertation, Indian Institute Technol. Jodhpur, India, 2021.

[4] A. Singh, A. Gupta, H. Wadhwa, S. Asthana, and A. Arora, "Temporal debiasing using adversarial loss based GNN architecture for crypto fraud detection," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2021, pp. 391–396.

[5] C. Prices, "Charts and market capitalizations | coinmarketcap. (SEM data)," CoinMarketCap, Online, Tech. Rep., 2022.

[6] K. Lašas, G. Kasputytė, R. Užupytė, and T. Krilavičius, "Fraudulent behaviour identification in Ethereum blockchain," in *Proc. CEUR Workshop, Inf. Soc. Univ. Stud.*, Kaunas, Lithuania, 23, Apr. 2020, pp. 1–8.

[7] J. T. Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, and M. Vasek, "An examination of the cryptocurrency pump-and-dump ecosystem," *Inf. Process. Manag.*, vol. 58, no. 4, Jul. 2021, Art. no. 102506.

[8] U. W. Chohan, "Are cryptocurrencies truly trustless?" in *Cryptofinance and Mechanisms of Exchange*. Berlin, Germany: Springer, 2019, pp. 77–89.

[9] H. Nghiem, G. Muric, F. Morstatter, and E. Ferrara, "Detecting cryptocurrency pump-and-dump frauds using market and social signals," *Exp. Syst. Appl.*, vol. 182, Nov. 2021, Art. no. 115284.

[10] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Jul. 2018, pp. 122–128.

[11] A. Trozze, J. Kamps, E. A. Akartuna, F. J. Hetzel, B. Kleinberg, T. Davies, and S. D. Johnson, "Cryptocurrencies and future financial crime," *Crime Sci.*, vol. 11, no. 1, pp. 1–35, Dec. 2022.

[12] F. Leal, A. E. Chis, and H. González–Vélez, "Multi-service model for blockchain networks," *Inf. Process. Manag.*, vol. 58, no. 3, May 2021, Art. no. 102525.

[13] *Top 10 Cryptocurrencies Price Analysis | Cointelegraph*. Accessed: Jul. 22, 2022. [Online]. Available: https://cointelegraph.com/category/top-10-cryptocurrencies

[14] J. Barna, "Blockchain and cryptocurrencies," Harvard Model Congr., Boston, MA, USA, Tech. Rep., 2022.

[15] B. B. Zarpelão, R. S. Miani, and M. Rajarajan, "Detection of Bitcoin-based botnets using a one-class classifier," in *Proc. IFIP Int. Conf. Inf. Secur. Theory Pract.* Cham, Switzerland: Springer, 2018, pp. 174–189.

[16] M. Bhowmik, T. S. S. Chandana, and B. Rudra, "Comparative study of machine learning algorithms for fraud detection in blockchain," in *Proc. 5th Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Apr. 2021, pp. 539–541.

[17] D. Sanz-Bas, C. del Rosal, S. L. Náñez Alonso, and M. Á. E. Fernández, "Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain," *Laws*, vol. 10, no. 3, p. 57, Jul. 2021.

[18] J. J. Castonguay and S. S. Smith, "Digital assets and blockchain: Hackable, fraudulent, or just misunderstood?" *Accounting Perspect.*, vol. 19, no. 4, pp. 363–387, Dec. 2020.

[19] L. Chen, J. Peng, Y. Liu, J. Li, F. Xie, and Z. Zheng, "Phishing scams detection in Ethereum transaction network," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–16, Feb. 2021.

[20] H. Arimura, M. Soufi, H. Kamezawa, K. Ninomiya, and M. Yamada, "Radiomics with artificial intelligence for precision medicine in radiation therapy," *J. Radiat. Res.*, vol. 60, no. 1, pp. 150–157, Jan. 2019.

[21] A. G. Luchkin, O. L. Lukasheva, N. E. Novikova, V. A. Melnikov, A. V. Zyatkova, and E. V. Yarotskaya, "Cryptocurrencies in the global financial system: Problems and ways to overcome them," in *Proc. Russian Conf. Digit. Economy Knowl. Manag. (RuDEcK)*, 2020, pp. 423–430.

[22] E. Jung, M. Le Tilly, A. Gehani, and Y. Ge, "Data mining-based Ethereum fraud detection," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 266–273.

[23] R. Bratspies, "Cryptocurrency and the myth of the trustless transaction," *Michigan Technol. Law Rev.*, vol. 25, no. 1, 2018.

[24] J. Cárdenas-Rodríguez, M. Restrepo Sierra, and D. Plazas Escudero, "Cryptocurrency scams," CLADS XVI, Puebla, Mexico, Tech. Rep., Jan. 2018.

[25] R. Tan, Q. Tan, P. Zhang, and Z. Li, "Graph neural network for Ethereum fraud detection," in *Proc. IEEE Int. Conf. Big Knowl. (ICBK)*, Dec. 2021, pp. 78–85.

[26] R. M. Aziz, M. F. Baluch, S. Patel, and A. H. Ganie, "LGBM: A machine learning approach for Ethereum fraud detection," *Int. J. Inf. Technol.*, vol. 14, no. 7, pp. 3321–3331, Dec. 2022, doi: 10.1007/s41870-022-00864-6.

[27] E. Grossi and M. Buscema, "Introduction to artificial neural networks," *Eur. J. Gastroenterol. Hepatol.*, vol. 19, pp. 1046–1054, Jan. 2008.

[28] H. H. S. Yin, K. Langenheldt, M. Harlev, R. R. Mukkamala, and R. Vatrapu, "Regulating cryptocurrencies: A supervised machine learning approach to de-anonymizing the Bitcoin blockchain," *J. Manage. Inf. Syst.*, vol. 36, no. 1, pp. 37–73, Jan. 2019.

[29] *Coinbase—Buy & Sell Bitcoin, Ethereum, and More With Trust*. Accessed: Jul. 22, 2022. [Online]. Available: https://www.coinbase.com/

[30] J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, "Who are the phishers? Phishing scam detection on Ethereum via network embedding," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 2, pp. 1156–1166, Feb. 2022.

[31] A. Kumar, K. Abhishek, P. Nerurkar, M. R. Ghalib, A. Shankar, and X. Cheng, "Secure smart contracts for cloud-based manufacturing using Ethereum blockchain," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 4, p. e4129, Apr. 2022.

[32] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, and Y. Liu, "Transaction-based classification and detection approach for Ethereum smart contract," *Inf. Process. Manag.*, vol. 58, no. 2, Mar. 2021, Art. no. 102462.

[33] Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang, and X. Zhang, "Detecting phishing scams on Ethereum based on transaction records," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Oct. 2020, pp. 1–5.

[34] R. F. Ibrahim, A. M. Elian, and M. Ababneh, "Illicit account detection in the Ethereum blockchain using machine learning," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 488–493.

[35] W.-J. Tsaur, J.-C. Chang, and C.-L. Chen, "A highly secure IoT firmware update mechanism using blockchain," *Sensors*, vol. 22, no. 2, p. 530, Jan. 2022.

[36] W. Chen, Z. Zheng, E. C.-H. Ngai, P. Zheng, and Y. Zhou, "Exploiting blockchain data to detect smart Ponzi schemes on Ethereum," *IEEE Access*, vol. 7, pp. 37575–37586, 2019.

[37] V. Lee and H. Wei, "Exploratory simulation models for fraudulent detection in Bitcoin system," in *Proc. IEEE 11th Conf. Ind. Electron. Appl. (ICIEA)*, Jun. 2016, pp. 1972–1977.

[38] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust Bitcoin fraud detection," in *Proc. Inf. Secur. South Afr. (ISSA)*, 2016, pp. 129–134.

[39] S. Sayadi, S. B. Rejeb, and Z. Choukair, "Anomaly detection model over blockchain electronic transactions," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 895–900.

[40] B. Chen, F. Wei, and C. Gu, "Bitcoin theft detection based on supervised machine learning algorithms," *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, Feb. 2021.

[41] A. Kasera, "Cryptocurrency frauds," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 6, pp. 261–268, Aug. 2020, doi: 10.35940/ijeat.F1391.089620.

[42] G. D. Arya, K. V. S. Harika, D. V. Rahul, S. Narasimhan, and A. Ashok, "Analysis of unsupervised learning algorithms for anomaly mining with Bitcoin," in *Machine Intelligence and Smart Systems*. Berlin, Germany: Springer, 2021, pp. 365–373.

[43] T. Pham and S. Lee, "Anomaly detection in the Bitcoin system—A network perspective," 2016, *arXiv:1611.03942*.

[44] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," *Exp. Syst. Appl.*, vol. 150, Jul. 2020, Art. no. 113318. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417420301433

[45] L. Rokach and O. Maimon, "Decision trees," in *Data Mining and Knowledge Discovery Handbook* (Series in Machine Perception and Artificial Intelligence), vol. 81. Singapore: World Scientific, 2005, pp. 165–192.

[46] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001.

[47] T. Evgeniou and M. Pontil, "Support vector machines: Theory and applications," in *Machine Learning and Its Applications, Advanced Lectures*, vol. 2049. Springer, 2001, pp. 249–257.

[48] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," 2015, *arXiv:1511.08458*.

[49] C. Zhang and Y. Ma, *Ensemble Machine Learning: Methods and Applications*. Berlin, Germany: Springer, 2012.

[50] T. M. Khoshgoftaar, J. Van Hulse, and A. Napolitano, "Comparing boosting and bagging techniques with noisy and imbalanced data," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 41, no. 3, pp. 552–568, May 2011.
[51] *Ethereum Fraud Detection Dataset*. Accessed: Jul. 18, 2023. [Online]. Available: https://www.kaggle.com/datasets/vagifa/ethereum-frauddetection-dataset?resource=download
[52] L. Perez and J. Wang, "The effectiveness of data augmentation in image classification using deep learning," 2017, *arXiv:1712.04621*.
[53] C. C. Aggarwal, A. Hinneburg, and D. A. Keim, "On the surprising behavior of distance metrics in high dimensional space," in *Database Theory—ICDT*, J. Van den Bussche and V. Vianu, Eds. Berlin, Germany: Springer, 2001, pp. 420–434.

QASIM UMER received the B.S. degree in computer science from Punjab University, Pakistan, in 2006, the M.S. degree in .Net distributed system development and the M.S. degree in computer science from the University of Hull, U.K., in 2009 and 2013, respectively, and the Ph.D. degree from the Beijing Institute of Technology, China. He is an Assistant Professor with the Department of Computer Sciences, COMSATS University Islamabad, Vehari Campus, Pakistan. He is particularly interested in machine learning, data mining, and software maintenance. He is also interested in developing practical tools to assist software engineers.

JIAN-WEI LI received the master's degree in psychology and Ph.D. degree in pedagogy. He is an Associate Professor and master's supervisor of the School of Marxism of Zhejiang Gongshang University, and a doctoral candidate of the Education Research Institute of Xiamen University. His research interests include but are not limited to deep learning for students, teacher development literacy in the digital era, and the construction of teacher–student relationships.

MUHAMMAD REHAN ASHRAF received the M.Sc. and M.Phil. degrees from Quaid-I-Azam University, Islamabad, Pakistan. He is an Assistant Professor with the Department of Computer Science, COMSATS University Islamabad, Vehari Campus, Pakistan. He is particularly interested in machine learning, data mining, and digital image processing.

RAB NAWAZ BASHIR received the Ph.D. degree in computer science and the M.S. degree in computer science from The Islamia University Bahawalpur, Bahawalpur, Pakistan, in 2015 and 2021, respectively. He is currently a Lecturer with COMSATS University Islamabad, Vehari, Pakistan. His research interest includes the Internet of Things (IoT) applications in agriculture.

HAMID GHOUS is the Head of Research for the Computer Science Department with the Institute of Southern Punjab (ISP). He is also leading the Vision, Linguistic, and Machine Learning Laboratory, ISP. He has authored and coauthored more than 30 publications in the past. His main area of research is machine and deep learning methods.