International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 4, August, 2023, pp. 931-937
Journal homepage: http://iieta.org/journals/isi

Hybrid Deep Learning Approach Utilizing RNN and LSTM for the Detection of DDoS Attacks Within the Bitcoin Ecosystem

Amenah Abdulabbas Almamoori[1*], Wesam Samer Bhaya[2]

[1] Department of Information Networks, College of Information Technology, University of Babylon, Babylon 51001, Iraq
[2] Department of Information Security, Faculty of Information Technology, University of Babylon, Babylon 51001, Iraq

Corresponding Author Email: amenah.net.phd@student.uobabylon.edu.iq

https://doi.org/10.18280/isi.280413

Received: 26 May 2023
Revised: 18 August 2023
Accepted: 23 August 2023
Available online: 31 August 2023

Keywords:
blockchain, cryptocurrency exchange, deep learning, Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Conditional Table Generative Adversarial Network (CTGAN)

ABSTRACT

The recent surge in the attention garnered by blockchain technology, an immutable ledger enabling decentralized transactions, is noteworthy. However, the security of blockchain remains susceptible to various attacks, including distributed denial-of-service (DDoS) attacks, which have increasingly targeted Bitcoin services. In response, deep learning algorithms have emerged as a potent solution to complex problems within the realm of information science. This study proposes a novel approach, utilizing these algorithms within hybrid frameworks, to address intricate cybersecurity issues. The methodologies were implemented and fine-tuned within a Python environment. Initially, a technique known as data augmentation was applied to an experimental domain aimed at verifying efficiency and boosting precision in complex datasets. Data augmentation, a method of generating new data points from existing ones, artificially enhances the volume of data. A Conditional Table Generative Adversarial Network (CTGAN) approach was adopted for the creation of tabular synthetic data. The utilization of synthetic data was found to enhance the model's performance and robustness compared to the exclusive use of original data. Subsequently, a binary classification hybrid deep learning model, incorporating Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) algorithms, was proposed for the detection of DDoS attacks within cryptocurrency networks. The proposed model was then validated using actual instances of DDoS attacks within the Bitcoin service dataset. The validation process incorporated a test set comprising 20% of the augmented data. Evidently, the proposed model outperformed standard deep learning implementations, achieving an impressive accuracy of approximately 95.84%. This study, therefore, presents a promising approach to mitigating DDoS attacks within the Bitcoin ecosystem.

1. INTRODUCTION

The advent of digital currencies, or cryptocurrencies, has precipitated the emergence of blockchain technology, an essential component for their operation. The sudden surge in the value of these digital currencies has led to the establishment of cryptocurrency exchanges, online platforms facilitating the storage, purchase, and sale of cryptocurrencies. Examples of these cryptocurrencies include Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Ripple (XRP), and Libra [1, 2].

At the core of these systems is the blockchain, a data structure and distributed ledger technology (DLT) that employs an unalterable cryptographic signature, known as a hash, to chronicle transactions. DLT participants, who manage this decentralized database, are widely recognized. One of the primary functions of the blockchain is to record cryptocurrency transaction data. For this operation, a peer-to-peer network is needed, ensuring that every user within the network has access to all transactional information. The operation of the blockchain can be conceptualized into five key components: database, block, hash, miner, transaction, and consensus mechanism [3].

However, as the blockchain ecosystem matures and new applications are unearthed, organizations across various industries are confronted with a complex and potentially intricate set of challenges, alongside emerging dependencies. Bitcoin, with the highest trading volume of any cryptocurrency, has also been a prime target for vulnerabilities and attacks, such as distributed denial-of-service (DDoS) attacks, as the Bitcoin market expands [4]. A DDoS attack, a significant network threat, rapidly depletes the resources of its targets by flooding the victim's network infrastructure with spurious requests. Consequently, the website becomes virtually inaccessible for intended users [5].

A fundamental issue within DDoS attack detection techniques is the apparent disregard for the constraints of real-time problems and small datasets. A thorough understanding of the application of emerging technologies is required to enhance efficiency. To date, research efforts have primarily focused on different DDoS detection techniques or incorporated some aspects of blockchain-based research for a specific domain using the same datasets available in research engines.

Thus, this paper intends to address this knowledge gap by exploring innovative and effective detection solutions. Notably, CTGAN outperforms most other methods on real datasets, where other deep learning methods fall short. In this paper, CTGAN was employed for data augmentation, and a hybrid deep learning technique utilizing two deep neural network models was proposed for DDoS attack detection. The contributions of the proposed model are as follows:

•Dataset preparation for DDoS attacks on Bitcoin.

•Dataset pre-processing.

•Utilization of CTGAN for data augmentation to enhance accuracy and effectively reduce execution time.

•Proposal of a hybrid deep learning model deploying a Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) for DDoS attack detection in cryptocurrency networks.

•Demonstration of robust detection accuracy for DDoS attacks through comprehensive experimental findings.

The remainder of this paper is structured as follows: Section 2 reviews related works. Section 3 provides a detailed description of the proposed hybrid model, the dataset used in our study, and the pre-processing methods employed. Section 4 presents the experimental results, the performance metrics applied in this study, the performance of our proposed model, and a comparison with other similar models and studies. Section 5 discusses our work, followed by the conclusion in Section 6.

2. RELATED WORKS

This section synthesizes scholarly contributions on the detection and classification of Distributed Denial of Service (DDoS) attacks in cryptocurrency trading systems, specifically focusing on the application of artificial intelligence, including deep learning methodologies. The impacts of DDoS attacks on such systems are also examined.

In their seminal work, Vasek et al. [6] embarked on an empirical exploration of DDoS attacks within the Bitcoin ecosystem. Using the Mt. Gox exchange as a case study, they analyzed and compiled posts on the popular forum bitcointalk.org, specifically posts mentioning 'ddos', from May 2011 to October 2013. They employed a straightforward word-based classifier to identify threads associated with DDoS attacks, yielding a precision of 54%, a recall of 74%, and an overall accuracy of 75%. Their findings revealed DDoS attacks targeted against approximately 7.4% of Bitcoin-associated services.

Furthering this line of investigation, Feder et al. [7] analyzed the impact of DDoS attacks on cryptocurrency exchanges, with an emphasis on the Mt. Gox exchange, which experienced repeated DDoS attacks leading to its eventual shutdown due to a serious security breach. The researchers constructed an array of regressions to quantify the repercussions of such shocks on transaction volumes. Their regression model demonstrated significant results across varying specifications, indicating a decrease in high-volume trades in the aftermath of a DDoS attack. They further postulated that similar impacts could be observed from other classes of security breaches.

A novel transaction history summarization technique was proposed by Toyoda et al. [8], laying the groundwork for a multi-class service identification system for Bitcoin addresses. They argued that such a categorization system could offer significant benefits, including enhanced fraud detection capabilities. They introduced two methods for extracting transaction history, namely, address-based and owner-based methods. A random forest algorithm was employed for detection, achieving accuracies of 72% and 70% for the owner-based and address-based methods, respectively.

Dragomiretskiy [9] examined the financial implications of a DDoS attack on the Bitfinex exchange, a platform that derives revenue from transaction fees. The study invoked statistical techniques to evaluate the impacts of 18 DDoS attacks on the Bitfinex platform. Despite employing a sophisticated prediction model for the number of trades, the study found no significant disruption to trading activity on the exchange in the days following a DDoS attack.

Lastly, Abhishta et al. [1] conducted an assessment of the impacts of DDoS attacks on Bitfinex in the years 2016 to 2018. They predicted the average volume of Bitcoin traded on the exchange using an additive model and compared the goodness of fit of two models, linear OLS and quadratic OLS, to identify the superior estimation model. Their research suggested that the exchange could typically recover from a DDoS attack within a day. However, prolonged attacks could significantly affect the exchange's revenue streams.

In the realm of DDoS attack detection, Baek et al. [4] postulated a correlation between service- and network-level data DDoS attacks in Bitcoin. Real-world DDoS attack data on Bitcoin-related services were collected and analyzed. A methodology was proposed for delineating data that could be sourced from the Bitcoin network as well as block statistical data. The researchers then focused on employing deep learning techniques, such as multi-layer perceptron (MLP) detection and principal component analysis feature extraction, for the detection of DDoS attacks at the Bitcoin service level.

Data augmentation, a strategy that can enhance the resilience and performance of machine learning and deep learning models, is particularly beneficial in scenarios where high-quality data is scarce. In response to the challenge of generating realistic synthetic tabular data, due to inherent structural constraints and dependencies, Xu et al. [10] introduced CTGAN, a Generative Adversarial Network (GAN)-based solution. CTGAN harnessed the potential of GANs to learn and mimic the underlying data distribution, thereby facilitating the generation of data samples that closely resemble the original. A conditional framework was integrated into CTGAN, enabling the generation of samples based on specific attribute values, thus making it apt for tasks necessitating synthetic data with certain characteristics. The authors applied CTGAN to various real-world tabular datasets, such as credit card transactions and census income data, and found it to be successful in generating synthetic samples that closely matched the statistical properties of the real data. Comparative analysis with other baseline methods confirmed CTGAN's superiority in generating high-quality synthetic tabular data.

While numerous detection approaches for DDoS attacks have been proposed, many neglect to consider critical factors such as dataset size, complexity limitations, and real-time problem solving. The current paper aligns with these measurement studies, yet deviates in its proposition of a hybrid intelligent model for detecting DDoS attacks on cryptocurrency exchanges. This model leverages the combined potency of Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) algorithms for detection.

This proposed model distinguishes itself from the referenced studies through its utilization of hybrid deep learning methodologies and the application of data augmentation techniques. The upcoming sections will delve deeper into the specifics of this novel approach, and its potential contributions to the field of DDoS attack detection and prevention in cryptocurrency exchanges.

3. METHODOLOGY

This section describes and evaluates our method to detect DDoS attacks.

3.1 Dataset overview

The dataset applied in this paper was real cases of DDoS on Bitcoin services. Mt. Gox is responsible for several Bitcoin transactions. This paper used a case study for DDoS attacks on currency exchanges related to Mt. Gox. The data utilized in the previous DDoS attack research6 were downloaded from Vasek et al. [6]. DDoS attack data for this site are reported cases from May 2011 to October 2013. The DDoS attack data contain the following features: 'cat1', 'cat2', 'URL', 'name', 'IP', 'cf', 'ec2', 'incapsula' and 'DDoS'. Furthermore, all posts on the website containing the term 'DDoS' appeared between February 2011 and October 2013. Given that the Google API only returns the top 100 results, we issued requests at week-long intervals. The API returned the maximum 100 results in only 3 weeks (April and May 2013). In some circumstances, we shortened the time interval to ensure that all results including 'ddos' were obtained.

3.2 DDoS attacks detection model

The proposed model uses Bitcoin data to predict the DDoS attack that occurred in Bitcoin services. The outline of the proposed model is as follows:

(1) Dataset Reading: We retrieved the file containing the dataset to be processed and applied to the suggested model.

(2) Dataset Preprocessing: The samples from the dataset were analyzed by applying the following pre-processing steps:

•Data Encoding: Data were categorized into three types: structured, semi-structured and unstructured data. In the beginning, the model handled the issue of missing values in the dataset. In data encoding, we used the function LabelEncoder to normalize labels. It may also convert non-numerical labels to numerical ones. Missing values were processed, and null features were removed.

•Data scaling: Scaling data allowed the model to learn and comprehend the situation. Neural networks are an excellent example of what might happen when independent values are spread and processed without scaling. The most common techniques of feature scaling are standardization and normalization. Machine learning scaling is a technique used in data preparation that brings data points far apart closer together to improve the algorithm's performance and speed up the machine learning processing. In our model the data's range is scaled to [0, 1]. A min-max scaling is performed as follows:

$$Xsc = \frac{X - Xmin}{Xmax - Xmin} \qquad (1)$$

where, *Xmin* and *Xmax* represent the minimum and maximum values of every feature, respectively. After that, 80% of the data were randomly selected for training, whereas the remaining 20% were retained and used for testing evaluation.

•Data augmentation: A data augmentation technique was used to increase the number of samples for training a neural network. The technique generated new data from the original data. The data augmentation field is not new, and several data augmentation techniques have been applied to specific problems [11]. Previous studies have been conducted in the field of image processing, but our approach was applied to the real datasets in DDoS attacks on cryptocurrency networks. For instance, we proposed different approaches to data augmentation by using CTGAN. This basic way of increasing data was used in small datasets to combat overfitting [12]. We generated a new dataset with a DDoS attack to balance the original data, increase its size, prevent model from overfitting and improve model prediction success. The size of the original data was 1290 samples, and the size of the synthetic data points generated was 1000 samples. Therefore the data became 1243 for benign data and 1047 for DDoS attacks data.

(3) Data splitting: Data splitting is a significant aspect of data science in which data are divided into two or more subsets. Typically, in this study, we split the data into two-part splits; one part was used to evaluate or test the data with a test size of 20%, and the other was used to train the model.

(4) Hybrid Model: In the hybrid phase, we initially built a robust hybrid model by applying one layer of the RNN and five layers of LSTM. The practical phases of the proposed model for deep learning classification are shown in Figure 1. Predominantly, LSTM is a sophisticated deep RNN approach built primarily to handle the vanishing gradient problems that frequently emerge when learning long-term correlations between scope inputs and target outputs in artificial neural networks [13]. A cell, an input gate, an output gate and a forget gate are the four major components of an LSTM unit. The cell remembers values across variable time intervals, and the cell gates control the information that passes through it. The LSTM framework is composed of memory blocks that are linked together in recurrent networks. Furthermore, the memory block's objective is to maintain its state over time while regulating information flow using non-linear gate units [14].

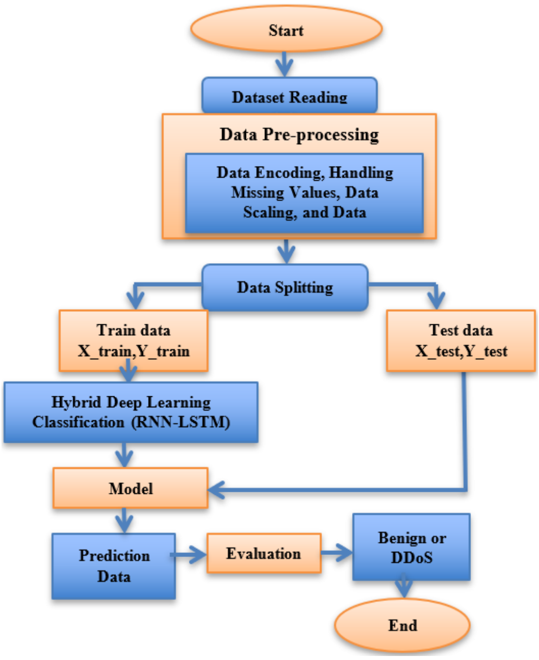

Start
Dataset Reading
Data Pre-processing
Data Encoding, Handling Missing Values, Data Scaling, and Data
Data Splitting
Train data X_train,Y_train
Test data X_test,Y_test
Hybrid Deep Learning Classification (RNN-LSTM)
Model
Prediction Data
Evaluation
Benign or DDoS
End

Figure 1. Proposed hybrid model for DDoS attack detection

RNN is one of the potential deep learning models, which is an excellent learning method for processing sequential data, such as speech recognition and language processing. It learns its features for time series data by storing past inputs in the internal representation of the neural network. Moreover, depending on previous and present data, RNN may predict future results.

Unfortunately, given the gradient exploding or gradient vanishing issue in the RNN structure, learning stored data for a long time can be challenging [15, 16]. The proposed system provided a hybrid deep learning approach for building and training a complex neural network model using the Keras API. This model is a hybrid architecture that combines SimpleRNN and multiple LSTM layers with additional components such as dropout and dense layers. The model is compiled with the Adam optimizer and uses mean squared error (MSE) as the loss function, with accuracy as the evaluation metric [17, 18].

The main steps of the model architecture can be summarized as follows:

(1) Sequential: This creates a linear stack of layers in Python, where you can add layers one after the other.

(2) SimpleRNN: The first layer is a SimpleRNN layer with 128 units, returning sequences, and using the ReLU activation function.

(3) Dropout: A dropout layer is added with a dropout rate of 0.2, which helps prevent overfitting by randomly dropping out a portion of the neurons during training.

(4) Multiple LSTM Layers: Several LSTM layers are stacked on top of each other. Each LSTM layer has a different number of units and uses the hyperbolic tangent (tanh) activation function. These layers are designed to capture complex sequential patterns in the data.

(5) Dense: A dense layer with a single neuron and sigmoid activation is added. This layer is the output layer of the network.

(6) Model Compilation: The model is compiled using the Adam optimizer, which is an adaptive learning rate optimization algorithm. The loss function is set to mean squared error (MSE), and the metrics for evaluation are accuracy.

(7) Model Summary: The summary method is used to print a summary of the model's architecture to the console.

(8) Model Training: The model is trained using the fit function. The training data is provided along with batch size, number of epochs, and validation data. The steps per epoch parameter determines how many batches are processed per epoch.

4. RESULTS

In this section, experiments were conducted in Python and were repeated several times to select the best parameters for our proposed model.

Table 1 shows the results obtained through the implementation of several deep learning methods, the most important of which are RNN and LSTM, as well as the proposed hybrid model, namely, RNN-LSTM. The hybrid model achieved the highest performance rate compared with the other algorithms.

To prove the efficiency of the proposed hybrid model, several criteria were used, namely, accuracy, precision, recall, F1 score, Cohen's kappa coefficient and ROC AUC.

The rate at which a classifier properly labels occurrences is referred as prediction accuracy and is calculated as follows:

$$accuracy = \frac{tp + tn}{tp + tn + fp + fn} \tag{2}$$

Precision is a statistical variability metric that describes random errors and is calculated as follows:

$$precision = \frac{tp}{tp + fp} \tag{3}$$

Recall is the fraction of correctly anticipated positive cases from all positive instances and is calculated as follows:

$$recall = \frac{tp}{tp + fn} \tag{4}$$

F1 score is the mean of memory and accuracy. It combines the precision and recall scores of a model. This criterion is calculated as:

$$f1_{score} = \frac{2 \times precision \ \times recall}{precision + recall} \tag{5}$$

The present work achieves high accuracy, about 95% in comparison with other experimental studies by using the same dataset. Table 2 shows the accuracy of the detection of DDoS attacks in this proposed model and previous experiments.

Table 1. Comparative results for DDoS attack detection under different deep learning algorithms

	RNN	LSTM	Proposed Hybrid Model (RNN-LSTM)
Accuracy	0.919214	0.926100	0.958400
Precision	0.988636	0.960000	0.988827
Recall	0.832536	0.803828	0.846890
F1 score	0.903896	0.875000	0.912371
Cohen's kappa	0.835095	0.785985	0.848642
ROC AUC	0.912252	0.887858	0.916393

Table 2. Comparison of the proposed model for DDoS attack detection on Bitcoin with other experimental studies

Ref.	Published Year	Detection Methods	Accuracy Results
[6]	2014	Word-based classifier	75%
[4]	2019	Multi-Layer Perceptron(MLP)	50%
Proposed Hybrid Model		RNN-LSTM	95%

The accuracy of the proposed hybrid model is shown in Figures 2-4 present the accuracy of the RNN and LSTM algorithms, respectively.

Finally, confusion matrix was utilised to demonstrate the stability of the proposed hybrid model depending on the detection sensitivity of DDoS attacks.

TP and FN are the most fundamental metrics in attack detection, where TP is the number of attacks correctly classified as attacks, and FN is the number of attacks wrongly classified as benign records.

Furthermore, TN is the number of benign records correctly classified as benign records, and FP is the benign records wrongly classified as attacks (Eq. (6)).

The confusion matrix of the proposed hybrid model RNN-LSTM, RNN and LSTM algorithms is shown in Figures 5-7, respectively.

$$\begin{array}{cccc} & & \text{Predicted} & \\ & & \text{Positive} & \text{Negative} \\ \text{Actual} & \text{Positive} & \text{True Positive (TP)} & \text{False Positive (FP)} \\ & \text{Negative} & \text{False Negative (FN)} & \text{True Negative (TN)} \end{array} \tag{6}$$

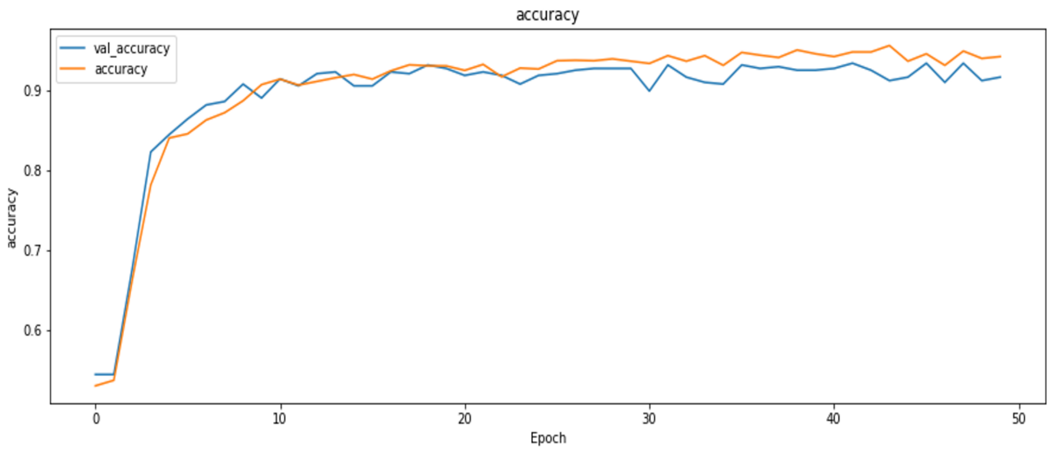


Figure 2. Accuracy of the proposed hybrid model (RNN-LSTM)

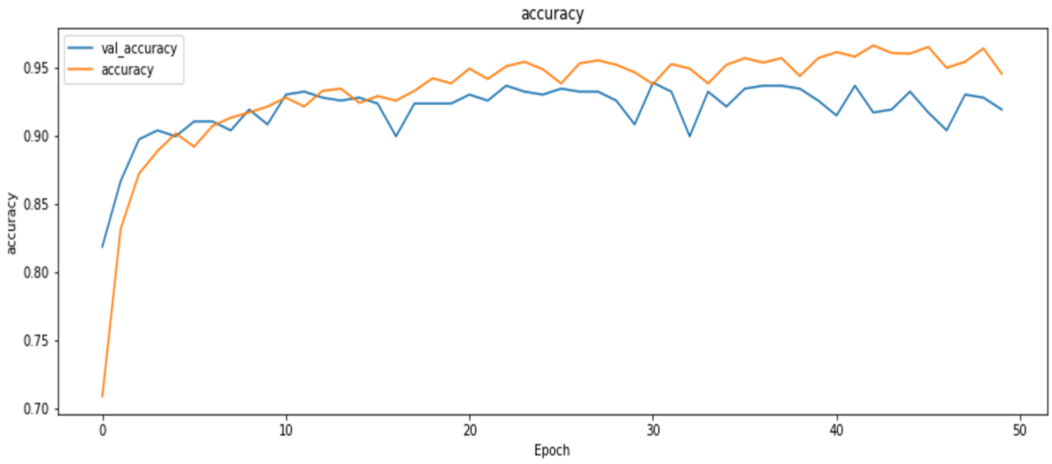


Figure 3. Accuracy of the RNN

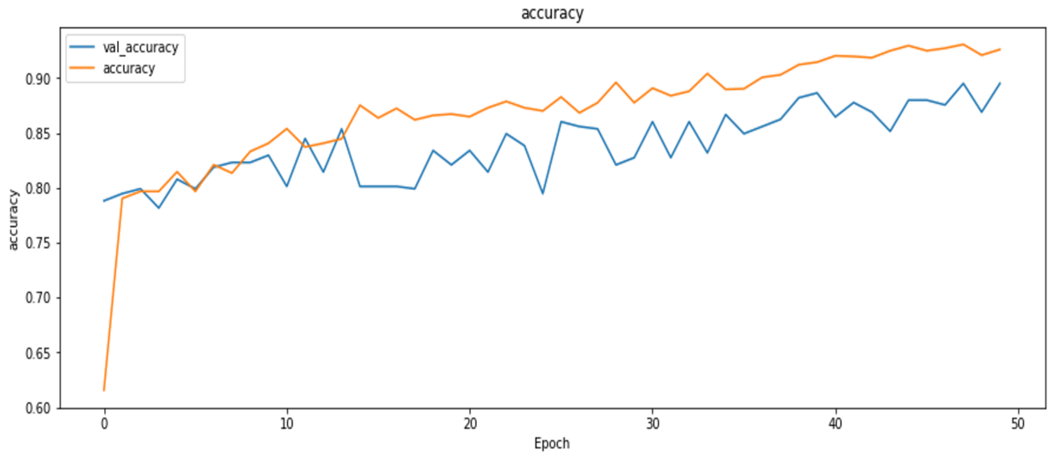
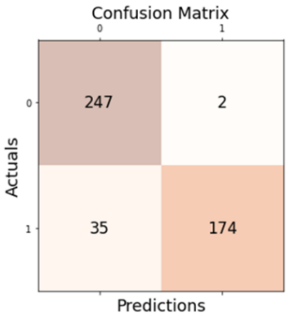
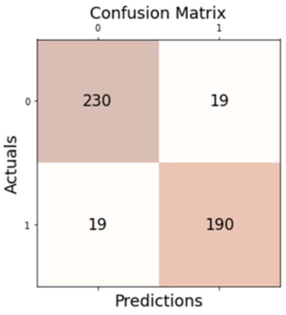


Figure 4. Accuracy of the LSTM


Confusion Matrix
0
1
0
1
Actuals
Predictions

	0	1
0	247	2
1	35	174

Figure 5. RNN-LSTM


Confusion Matrix
0
1
0
1
Actuals
Predictions

	0	1
0	230	19
1	19	190

Figure 6. RNN

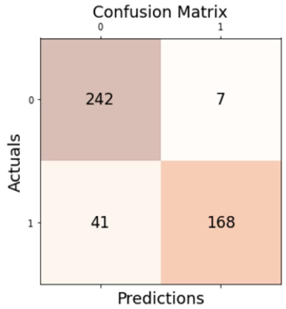


Figure 7. LSTM

A binary confusion matrix is a tool used in the field of machine learning and statistics to assess the performance of a binary classification model. It provides a comprehensive summary of how well the model has classified instances into two classes: usually a "positive" class and a "negative" class. The matrix is organized into four cells, each representing a different outcome based on the model's predictions and the actual ground truth. we can describe the content of a binary confusion matrix:

True Positives (TP): These are instances that the model correctly predicted as positive. In other words, the instances belong to the positive class and were classified as such by the model. These are cases where the model got it right.

False Positives (FP): These are instances that the model incorrectly predicted as positive. These instances actually belong to the negative class, but the model mistakenly classified them as positive. False positives are also known as Type I errors or "false alarms."

True Negatives (TN): These are instances that the model correctly predicted as negative. These instances belong to the negative class, and the model correctly identified them as such. True negatives represent cases where the model got the negative class prediction right.

False Negatives (FN): These are instances that the model incorrectly predicted as negative. These instances are actually part of the positive class, but the model erroneously classified them as negative. False negatives are also known as Type II errors or "missed opportunities."

5. DISCUSSION

The cybercriminal community profits from DDoS attacks. Now is the time to increase the performance of security measures and protect the security of consumer data. Deep learning scope provides a mechanism to solve complex problems in data security. Particularly, recurrent or very deep neural networks are difficult to train because of overfitting. Thus, to overcome this challenge, our research proposes a hybrid model by using LSTM with RNN. Recurrent generative adversarial artificial neural networks are distinguished by their interconnectedness of all neurons in the network, which, when grouped, forms an associative memory for network support. This property makes this type of network popular for associative memories. In addition to database size, an enormously significant issue is the balance between classes inside the bank, because the network can only 'learn' after successive presentations of various norms of all the judgments that the network must conduct. Data augmentation involves artificially increasing the diversity and quantity of training data by applying various transformations to the existing data. These transformations create new examples that are still consistent with the original data. Data augmentation can improve a model's performance by increasing diversity, reduced overfitting, invariant features learning, regularization, better generalization, solving data scarcity, and domain adaptation. Therefore, this research presents a way to balance the values by augmenting the size of the dataset to achieve high accuracy in detecting DDoS attacks in cryptocurrency networks.

6. CONCLUSION

In this paper, we proposed hybrid detection model based on deep learning algorithms, such as RNN and LSTM. In our scenario, the model used CTGAN to create tabular synthetic data using a conditional GAN. The results showed that the proposed hybrid model achieved high accuracy compared with other deep learning algorithms. When we compared the proposed model with previous studies that used the same dataset, we found that the model achieved the highest accuracy. The high accuracy of a proposed hybrid model in the field of cybersecurity could have significant implications for addressing DDoS (Distributed Denial of Service) attacks on cryptocurrency networks. The high accuracy of the hybrid model could impact the field of early detection and mitigation, reduce false positives, effective resource allocation, adaptive defense mechanisms, risk reduction for cryptocurrency transactions, improved reputation and trust, cost savings, and industry advancement. In the future, we would test the proposed system on a huge dataset to detect DDoS attacks on cryptocurrency and other applications of the blockchain network. Testing proposed systems on large datasets to detect Distributed Denial of Service (DDoS) attacks on cryptocurrency and other applications of blockchain networks is a proactive approach to ensuring the security and robustness of these systems. Also testing the effectiveness of response and mitigation strategies, such as rate limiting, traffic filtering, and traffic diversion, in mitigating the impact of DDoS attacks.

REFERENCES

[1] Abhishta, A., Joosten, R., Dragomiretskiy, S., Nieuwenhuis, L.J. (2019). Impact of successful ddos attacks on a major crypto-currency exchange. In 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Pavia, Italy, pp. 379-384. https://doi.org/10.1109/EMPDP.2019.8671642

[2] Sabry, F., Labda, W., Erbad, A., Malluhi, Q. (2020). Cryptocurrencies and artificial intelligence: Challenges and opportunities. IEEE Access, 8: 175840-175858. https://doi.org/10.1109/ACCESS.2020.3025211

[3] Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K.M., Almotairi, S., Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain-A comprehensive insight. Symmetry, 13(2): 227. https://doi.org/10.3390/sym13020227

[4] Baek, U.J., Ji, S.H., Park, J.T., Lee, M.S., Park, J.S., Kim, M.S. (2019). DDoS attack detection on bitcoin ecosystem using deep-learning. In 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, pp. 1-4.

https://doi.org/10.23919/APNOMS.2019.8892837

[5] Yin, H.S., Vatrapu, R. (2017). A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In 2017 IEEE international conference on big data (Big Data), Boston, MA, USA, pp. 3690-3699. https://doi.org/10.1109/BigData.2017.8258365

[6] Vasek, M., Thornton, M., Moore, T. (2014). Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. In Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, pp. 57-71. https://doi.org/10.1007/978-3-662-44774-1_5

[7] Feder, A., Gandal, N., Hamrick, J.T., Moore, T. (2017). The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. Journal of Cybersecurity, 3(2): 137-144. https://doi.org/10.1093/cybsec/tyx012

[8] Toyoda, K., Ohtsuki, T., Mathiopoulos, P.T. (2018). Multi-class bitcoin-enabled service identification based on transaction history summarization. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1153-1160. https://doi.org/10.1109/Cybermatics_2018.2018.00208

[9] Dragomiretskiy, S. (2018). The influence of DDoS attacks on cryptocurrency exchanges. Bachelor's thesis, University of Twente.

[10] Xu, L., Skoularidou, M., Cuesta-Infante, A., Veeramachaneni, K. (2019). Modeling tabular data using conditional gan. Advances in Neural Information Processing Systems 32 (NeurIPS 2019).

[11] Perez, L., Wang, J. (2017). The effectiveness of data augmentation in image classification using deep learning. arXiv preprint arXiv:1712.04621. https://doi.org/10.48550/arXiv.1712.04621

[12] Han, D., Liu, Q., Fan, W. (2018). A new image classification method using CNN transfer learning and web data augmentation. Expert Systems with Applications, 95: 43-56. https://doi.org/10.1016/j.eswa.2017.11.028

[13] Hochreiter, S., Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8): 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

[14] Van Houdt, G., Mosquera, C., Nápoles, G. (2020). A review on the Long Short-Term Memory model. Artificial Intelligence Review, 53: 5929-5955. https://doi.org/10.1007/s10462-020-09838-1

[15] Guesbaya, M., García-Mañas, F., Rodríguez, F., Megherbi, H. (2023). A soft sensor to estimate the opening of greenhouse vents based on an LSTM-RNN neural network. Sensors, 23(3): 1250. https://doi.org/10.3390/s23031250

[16] Yu, J., de Antonio, A., Villalba-Mora, E. (2022). Deep learning (CNN, RNN) applications for smart homes: A systematic review. Computers, 11(2): 26. https://doi.org/10.3390/computers11020026

[17] Bani, R., Amri, S., Zenkouar, L., Guennoun, Z. (2023). Deep neural networks for part-of-speech tagging in under-resourced Amazigh. Revue d'Intelligence Artificielle, 37(3): 611-617. https://doi.org/10.18280/ria.370310

[18] Patil, R.R., Kumar, S., Rani, R. (2022). Comparison of artificial intelligence algorithms in plant disease prediction. Revue d'Intelligence Artificielle, 36(2): 185-193. https://doi.org/10.18280/ria.360202