Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2023.037606
Article

Intelligent Financial Fraud Detection Using Artificial Bee Colony Optimization Based Recurrent Neural Network

T. Karthikeyan[1,*], M. Govindarajan[1] and V. Vijayakumar[2]

[1]Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India
[2]Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India
*Corresponding Author: T. Karthikeyan. Email: karthi4cse@gmail.com
Received: 10 November 2022; Accepted: 10 March 2023; Published: 23 June 2023

Abstract: Frauds don't follow any recurring patterns. They require the use of unsupervised learning since their behaviour is continually changing. Fraudsters have access to the most recent technology, which gives them the ability to defraud people through online transactions. Fraudsters make assumptions about consumers' routine behaviour, and fraud develops swiftly. Unsupervised learning must be used by fraud detection systems to recognize online payments since some fraudsters start out using online channels before moving on to other techniques. Building a deep convolutional neural network model to identify anomalies from conventional competitive swarm optimization patterns with a focus on fraud situations that cannot be identified using historical data or supervised learning is the aim of this paper Artificial Bee Colony (ABC). Using real-time data and other datasets that are readily available, the ABC-Recurrent Neural Network (RNN) categorizes fraud behaviour and compares it to the current algorithms. When compared to the current approach, the findings demonstrate that the accuracy is high and the training error is minimal in ABC_RNN. In this paper, we measure the Accuracy, F1 score, Mean Square Error (MSE) and Mean Absolute Error (MAE). Our system achieves 97% accuracy, 92% precision rate and F1 score 97%. Also we compare the simulation results with existing methods.

Keywords: Fraud activity; optimization; deep learning; classification; online transaction; neural network; credit card

1 Introduction

The current state of traditional commerce is changing as a result of virtual businesses and the internet. E-commerce has greater value now that there is a worldwide market, more freedom, and more competition. E-commerce also makes it simpler and more accessible to innovate in the banking and payment sectors. E-commerce makes life simple for users, whether they are consumers or business owners. It is important in the more competitive and global economy [1]. People are moving away from conventional markets and toward the growing global market. It has a variety of restrictions in addition

to providing customers with conveniences. For e-commerce or the digital market, online payment is essential [2].

The demand for the financial and banking sectors has grown as the size of the global market has expanded. With the use of smart devices like a laptop, mobile phone, desktop, personal digital assistance (PDA), etc., online payments enable you to conduct transactions from any location, at any time [3]. The elimination of traditional commerce's constraints is the primary driver of the expansion of electronic payments. The user may physically visit the bank to complete the transaction without having to wait in a big line. It offers a number of advantages, such as speedier transactions that may be completed in a matter of minutes without having to visit a bank or wait in line [4].

There are two methods of execution both online and offline electronic payments. Virtual payment may be recognized as online payment. Account holder name, Postal Index Number (PIN), card number, expiration date, and other sensitive details are needed for online payments [5]. Physical payment can be identified as offline payment. Cardholder presence and PIN are needed for offline payments. The first item needed for online payment fraud is a cardholder's credit card number. These frauds can be carried out in a variety of ways. Phishing, identity theft, skimming, using lost or stolen credit cards, card cloning, etc. are some common techniques for online credit card fraud [6].

In addition to these techniques, there are other systems that enable credit card fraud, such as malware or key loggers that may steal credit card information during an online transaction, or scanning equipment that can read your credit card information. Online payments make the procedure simpler even though they don't require a signature or your card's PIN information. Most websites steal card information and sell it to other parties; many fraudsters are active on the dark web, making them tough to catch [7,8]. There are several payment methods on the market that may be used for online purchases.

Depending on their needs and preferences, users use various payment methods. There are many different kinds of payment methods, including credit cards, debit cards, net banking, and electronic wallets. The danger associated with online payments is another reason why over 60% of Internet users still favor the Cash on Delivery (COD), payment method [9,10]. CC is a popular, widely used, and promising electronic payment method for online purchasing. As banks are giving customers credits for transactions that last a certain amount of time. Customer can choose to pay using CC with ease. Today, more people are using online payment methods [11]. The credit card is used both online and offline [12].

The Reserve Bank is attempting to strengthen security in light of the increasing incidence of cybercrimes. In particular, a digital transaction is seeing significant increase nowadays. The goal of the central bank is to improve cyber risk security [13]. This is to assure constant security in addition to the evolving types of security extortion on the internet. Electronic Commerce (E-Commerce) is widely available in the Indian market. It now offers facilities to organizations of all ages. Where customers may conveniently purchase online. In comparison to offline or conventional shopping methods, it offers the current generation additional advantages. E-commerce provides a vast array of options, amenities, discounts, and promotions [14]. The remainder of the article is organized as follows, the existing approaches are given in Section 2, the proposed methodology is elucidated in Section 3, the results are discussed in Section 4, and the article is concluded in Section 5.

2 Literature Review

India has tapped into the global market by attracting the interest of foreign businesses. Users' interest in online buying has risen due to additional facilities and offers [15]. In the digital world, fraud detection is seen as a critical procedure, and this article focuses on the classification of fraud activities. For the competitive swarm-based deep convolutional neural network-based categorization of legitimate and fraudulent transactions, an efficient optimization-based technique is created.

Sequence and static learners can achieve the credit card fraud classification [16]. The generalised adversarial network, which is based on deep learning, is used to perform the classification procedure [17]. Support vector machines, recurrent neural networks and Auto Encoder based Restricted Boltzmann Machines (AERBM) are deep learning- and machine learning-based approaches, respectively, that are used to classify credit card fraud [18].

Using a hybrid data resampling approach and a neural network ensemble classifier, an efficient method for identifying credit card fraud [19]. The ensemble classifier in the adaptive boosting (AdaBoost) method is built utilising a long short-term memory (LSTM) neural network as the basis learner. In the meanwhile, hybrid resampling is carried out using the edited nearest neighbour method and the synthetic minority oversampling methodology. The utility of the proposed strategy is demonstrated using publicly accessible real-world credit card transaction datasets. Machine learning (ML)-based methods for detecting fraudulent credit card transactions have been described in recent study, however their detection scores still need to be improved because of the imbalance of classes in any given dataset. A few approaches have generated remarkable results on diverse datasets [20].

Internet-enabled worldwide online communication has boosted credit card theft, which costs customers and financial institutions billions of dollars every year in lost revenue. The thieves always come up with new schemes to carry out illicit activities. Therefore, it is essential to combat fraud using novel detection methods in order to reduce these losses. This study describes the staking ensemble strategy for combining many classifiers to identify credit card fraud. The categorization method in the current system has the issue of being incapable of processing fast computation. Error frequency might result in misclassification. The current approach is inefficient due to the computational cost and accuracy. Low data amount and low training quality are both problems. An efficient recurrent neural network based on Artificial Bee Colony optimization is created by taking these limitations into account.

3 Existing System

The complexity of the network also rises as the number of levels develops. The depth of the network is often increased by adding more layers or recurrent connections, which enables the network to do "deep learning," or several degrees of feature extraction and data representation. The higher layers of these networks, which are often constructed from nonlinear but basic units, provide a more abstract representation of the data and reduce unwelcome variability. Recurrent Neural Networks (RNNs), which are Artificial Neural Network (ANN) with recurrent connections and can represent sequential input for sequence recognition and prediction, are a subclass of ANNs. High-dimensional hidden states with non-linear dynamics make up RNNs. The network's memory is implemented in the hidden state structure, and each layer's current state is dependent on its previous state.

The RNNs can store, recall, and process historical complicated signals for extended periods of time thanks to their structure. RNNs are able to predict the sequence in the following time step and transfer an input sequence to an output sequence in the present time step. RNN training has

greatly benefited from the development of back-propagation utilizing gradient descent (GD). The development of RNNs has advanced practically because of this straightforward training method.

Long Short Term Memory (LSTM) networks were introduced by and to estimate the sequence of transactions. LSTM improved accuracy in detecting offline transactions when cardholders are physically present at merchant sites when comparing to the basic classification of the Russian Federation. Manual feature merging routines are useful for both sequential and non-sequential training systems. After reviewing the true positives, it was found that both methodologies detect different types of fraud, indicates that both can be used together.

Scalable Real-time Fraud Finder which was a combination of Kafka, Spark and Cassandra and computer vision to eliminate imbalances, non-stationary attributes and feedback delays. Theirs experimental results on large databases of credit card transactions showed that their approach was accurate, efficient, and scalable on most transactions. Time series eigen sequences for transaction similarity, where the evaluated transactions sequence. A time simulation strategy in this context may be more robust to modest changes in actual purchasing behavior. LSTMs combined with SVMs were experimented with real-time credit card transactions. The research focused on making the right choices features, data pre-processing and evaluation metrics to provide a clear basis for comparison, where the latter will facilitate comparison of results obtained from oriented datasets. Large real-world transactional data sets have shown that their proposed technique significantly improves the accuracy of alerts, the key the concern of fraud investigations.

To detect behavioral patterns of fraud while learning labeled data and proposed a CNN for fraud detection where feature matrices represented large amounts of transactional data. CNN is used for estimation inactive patterns or patterns in the data and when tested on real bank transactions it was demonstrated that their technique outperformed many other existing approaches. The increase in activity in terms of online shopping makes it clear that users' transaction behavior is often different and their behaviours must be able to determine the variability of transactions. Conventional models are not enough for such consumers and therefore this work focuses on detecting fraudulent transactions based on a user's behaviours.

4 Proposed System

This section elaborates the process of feature selection and classification of credit card fraud activity. The significant features are reclaimed using artificial bee colony optimization approach that is utilized by the convolutional neural network for classification of credit card fraud. The Artificial Bee Colony (ABC) optimization algorithm is a new stochastic population based meta heuristics optimization algorithm. It is good in exploring the search space efficiently. It is based on the foraging behavior of the honey bees to explore the new food sources. The process of initialization is given as,

$$a_{mi} = l_i + rand\,(0, 1) * (u_i - l_i) \tag{1}$$

where the food sources are indicated by a_{mi}, the upper and lower bound is indicated as u_i *and* l_i, respectively. The phases of ABC optimization algorithm are,

Employee bee phase: The employee bees search for the food sources and bring the nectar from the food sources to their hives and perform a wangle dance in the dance area allocated in hive. The nearby source of food is given as,

$$b_{mi} = a_{mi} + \varnothing_{mi}\,(a_{mi} - a_{ki}) \tag{2}$$

where randomly opted source of food is indicated as a_{ki}, index is indicated as i, and the range of random number $\varnothing_{mi}$ is [−a, a]. A new source of food b_{mi} and its fitness is estimated whereby selection of greedy technique is employed among b_{mi} and a_{mi}.

Onlooker bee phase: The onlooker bees select the best employed bee having the highest nectar amount by the dance they perform. The bee which dances faster is the bee having large amount of nectar. The value of probability is expressed as,

$$p_m = \frac{fit_m\left(\vec{a_m}\right)}{\sum_{m=1}^{SN} fit_m\left(\vec{a_m}\right)} \tag{3}$$

Scout bee phase: The scout bee is the bee which explores new search space having the food source. Initial direction of food source is found by the scout bees which are followed by employed bees.

The ABC algorithm is good in exploration because of the scout bee phase with random search space of the problem domain but poor at exploitation and have slow convergence rate. In literature, standard ABC algorithm is improved by introducing randomization strategies to enhance the exploitation and exploration level. The ABC algorithm is suitable to find the optimal multicast tree satisfying the QoS constraint since they have the good exploration level. Since the ABC algorithm finds the global optimum in lesser time, it is highly applicable in large dynamic environments.

Algorithm 1. Proposed ABC for feature selection

Initialize the population of solutions $x_{i,j}$, i = 1 ... SN, j = 1 ... D
Evaluate the population
cycle = 1
repeat
Produce new solutions $\upsilon_{i,j}$ for the employed bees by using (2) and evaluate them
Apply the greedy selection process
Calculate the probability values $P_{i,j}$ for the solutions $x_{i,j}$ by (1)
Produce the new solutions $\upsilon_{i,j}$ for the onlookers from the solutions $x_{i,j}$ selected depending on $P_{i,j}$ and evaluate them
Apply the greedy selection process
Determine the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution $x_{i,j}$ by (3)
Memorize the best solution achieved so far
cycle = cycle + 1
until cycle = MCN

Finding the optimal multicast tree using ABC algorithm necessitates to find the path established by the bees with the minimum value for the objective function. Normally, the standard ABC algorithm helps in promoting good exploration level by handling the problems over entire search space. Mostly, ABC fits to any kind of optimization problem for exploring the feasible solution in a constraint time limit.

Deep learning and the creation of models that mimic the neuronal activity of the human brain both require RNNs. They differ from other kinds of artificial neural networks in that they employ feedback loops to digest a series of input that influences the final output, making them particularly

effective in use cases where context is essential for predicting an outcome. As a result of these feedback loops, information can endure. This phenomenon is frequently referred to as memory.

The majority of RNN use cases are associated with language models, where predicting the next letter in a word or the next word in a phrase depends on the information that comes before it. An RNN trained with Shakespearean works effectively produces Shakespeare-like text in an intriguing experiment. Writing is a sort of computational creativity performed by RNNs. The AI's knowledge of syntax and semantics acquired from its training set allows it to simulate human inventiveness.

From the first input to the final output, RNNs may process data. RNNs employ feedback loops, such as backpropagation via time, during the computational process to loop information back into the network, unlike feed-forward neural networks. RNNs can analyze sequential and temporal data because of the connections made by this between inputs.

As shown in Fig. 1a conventional RNN includes three layers: input, recurrent hidden, and output. N input units make up the input layer. A series of vectors during time t, such as $\{\ldots, x_{t-1}, x_t, x_{t+1} \ldots\}$, are the inputs to this layer, where $x_t = (x_1, x_2, \ldots, x_N)$. A weight matrix W_{IH} is used to determine the links between the input units of a fully connected RNN and the hidden units in the hidden layer. The hidden layer has M hidden units $h_t = (h_1, h_2, \ldots, h_M)$, that are connected to each other through time with recurrent. Small non-zero components can be used to initialize hidden units, which can boost the network's overall performance and stability.

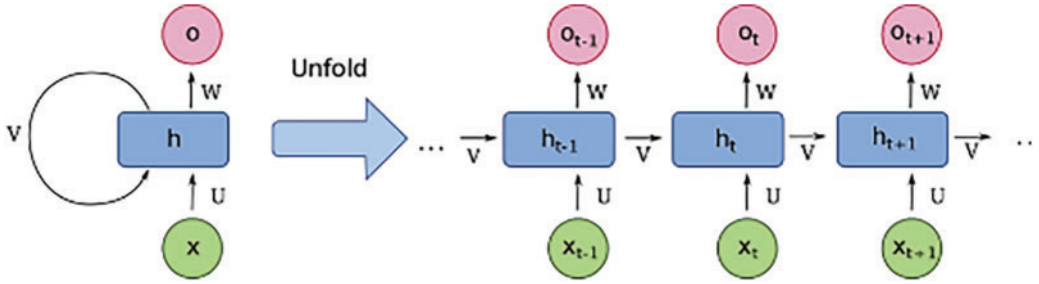

Figure 1: Architecture of recurrent neural network

The hidden layer defines the state space or "memory" of the system as

$$h_t = f_H(o_t) \tag{4}$$

where

$$o_t = W_{IH}x_t + W_{HH}h_t - 1 + b_h \tag{5}$$

$f_H(\cdot)$ is the hidden layer activation function, and b_h is the bias vector of the hidden units. The hidden units are connected to the output layer with weighted connections W_{HO}. The output layer has P units $y_t = (y_1, y_2 \ldots y_P)$ that are computed as

$$y_t = f_O(W_{HO}h_t + b_o) \tag{6}$$

where $f_O(\cdot)$ is the activation functions and b_o is the bias vector in the output layer. Since the input-target pairs are sequential through time, the above steps are repeated consequently over time $t = (1, \ldots, T)$.

Based on the input vector, the hidden states offer a prediction at the output layer for each time step. The hidden state of an RNN is a set of values that, independent of the influence of any external factors, compile all the specific knowledge required about the network's previous states over numerous time steps. At the output layer, this integrated information can define the network's future behaviour and produce precise predictions.

Multiple linear hidden layers function as a single linear hidden layer for linear networks. Since they can define nonlinear bounds, nonlinear functions are more potent than linear ones. The reason for learning input-target interactions in an RNN is the nonlinearity in one or more subsequent hidden layers. A popular option is the "sigmoid," which reduces a real value to the range [0, 1]. This activation function is typically applied in the output layer, where a classification model is trained using a cross-entropy loss function.

The "sigmoid" activation functions are defined as

$$б\,(x) = \frac{1}{1 + e^{-x}} \tag{7}$$

The issue and the type of data have a major impact on the activation function choice. "Sigmoid" activation functions rapidly saturate the neuron and can cause the gradient to disappear.

5 Dataset Description

All experiments are conducted in the Python environment, which takes center stage. The effectiveness of the suggested technique is examined in this part using three distinct datasets. Tables 1 to 3 provide a description of the dataset.

Table 1: Dataset description credit card fraud dataset

Description	Credit card fraud
Number of instances	58016
Number of attributes	40
Number class	2
Number of positive samples	57879
Number of negative samples	137

Table 2: Dataset description mortgage fraud dataset

Description	Mortgage fraud
Number of instances	48674
Number of attributes	11
Number class	2
Number of positive samples	48066
Number of negative samples	608

Table 3: Dataset description insurance fraud dataset

Description	Insurance fraud
Number of instances	44326
Number of attributes	39
Number class	2
Number of positive samples	43814
Number of negative samples	512

6 Metric Unit

Generally, the metrics in deep learning are meant for binary classification problems which shall be generalized for multiclass problems. For a multiclass classification problem, the metrics are performed as binary classifiers internally by assuming one class as positive and all other classes as negative, commonly known as one-*vs.*-all classifier.

Accuracy

Accuracy is the simplest and first metric which evaluates the performance of the network. It is calculated by number of correct predictions to the total predictions. It is represented by

$$\text{Accuracy} = \frac{\text{TP} + \text{True Negative (TN)}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{8}$$

Mean Absolute Error (MAE)

A measure of mistakes among paired observations describing the same phenomena is called mean absolute error. The MAE is expressed as,

$$\text{MAE} = \frac{\sum_{i=1}^{n} |l_i - m_i|}{n} \tag{9}$$

where prediction is given as l_i, true value is given as m_i and the total count of data point is given as n.

Mean Square Error (MSE)

The average of the squares of the mistakes, or the average squared difference between the estimated values and the actual value, is measured by the mean squared error or mean squared deviation of an estimator. MSE, which corresponds to the expected value of the squared error loss, is a risk function. The MSE is expressed as,

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n} \left(l_i - \widehat{l_i}\right)^2 \tag{10}$$

where observed range is indicated as l_i, predicted range is indicated as $\widehat{l_i}$, and count of data point is given as n.

F1-Score

F1-Score combines the precision and recall by calculating the weighted average of precision and recall. This score uses both false positives and false negatives for its calculation. F1-Score is more

informative measure than accuracy, mainly in case of imbalanced datasets. The estimation of F1 score is expressed as,

$$\text{F1score} = \frac{2 \times \text{Precison} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{11}$$

Precision

Precision deals with the frequency of the correct predictions of true positive out of total predictions. Recall deals with how many correct predictions are actually correct.

$$\text{Precision} = \frac{\text{True Positive}}{\text{Total Predicted Value}} \tag{12}$$

Recall

Recall is the percentage of successfully retrieved relevant documents in information retrieval.

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \tag{13}$$

7 Results and Discussion

In this section performance of the proposed approach is investigated with three different datasets. The performance is investigated in terms of Accuracy, f1 score, Mean Square Error (MSE) and Mean Absolute Error (MAE). The proposed ABC-RNN is compared with the existing technique RNN. The Performance of the proposed and existing techniques is given in Table 4.

Table 4: Comparison of performance for credit card fraud dataset

Technique	Accuracy (%)	MAE	MSE	Precision (%)	Recall (%)	F1_score (%)
RNN	90.26	0.357	0.399	88.07	89.11	85.58
ABC-RNN	96.03	0.205	0.360	97.04	93.40	91.98

Fig. 2 and Table 4 illustrate the comparison of accuracy, MAE, and MSE, precision, Recall and F1_Score for the credit card fraud detection. Fig. 2 shows a thorough analysis of the ABC_RNN model's accuracy, mean absolute error, and mean squared error, Precision, Recall and F1_Score in comparison to the RNN model that is currently in use on the Credit card Dataset. The resulting figures showed that the ABC-RNN model had enhanced accuracy of 96.03 percent, a lowered MAE of 0.205, a lower MSE of 0.360, precision of 97.04 percent, Recall of 93.04 and F1_Score of 91.98 compared to the RNN model's slightly decreased accuracy of 90.06 percent, increased MAE of 0.357, a increased MSE of 0.339, precision of 88.07 percent, Recall of 89.11 and F1_Score of 85.58.

The comparison of accuracy, MAE, and MSE, precision, recall, and F1 Score for credit card fraud detection is shown in Fig. 2 and Table 5. The accuracy, mean absolute error, mean squared error, precision, recall, and F1 Score of the ABC RNN model in comparison to the RNN model currently being used on the Credit card Dataset are all thoroughly analysed in Fig. 2. In comparison to the RNN model, which had slightly lower accuracy of 91.14 percent, higher MAE of 0.468, higher MSE of 0.379, precision of 90.59 percent, Recall of 89.11, and F1 Score of 86.81, the ABC-RNN model had improved accuracy of 98.60 percent, a lower MAE of 0.169, a lower MSE of 0.118, and precision of 98.78 percent, Recall of 92.08 and F1_Score of 94.21.

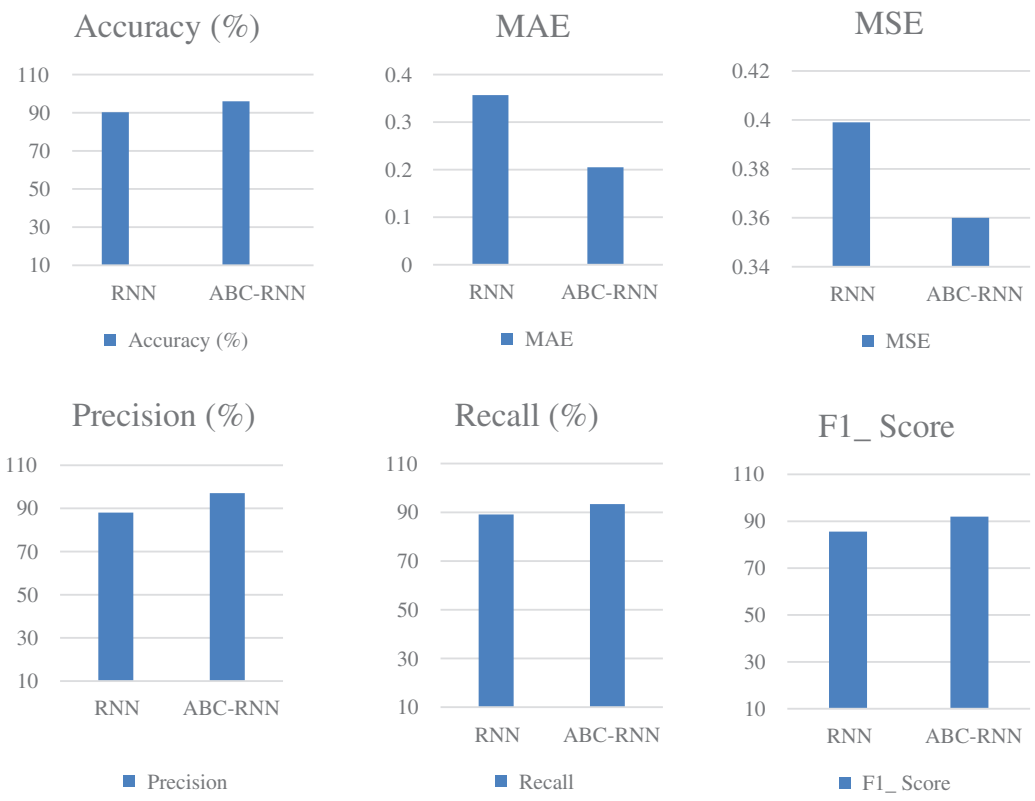

Figure 2: Comparison of performance for credit card fraud dataset

Table 5: Comparison of performance for insurance fraud dataset

Technique	Accuracy (%)	MAE	MSE	Precision (%)	Recall (%)	F1_score (%)
RNN	91.14	0.468	0.379	90.59	89.11	86.81
ABC-RNN	98.60	0.169	0.188	98.78	92.08	94.21

The comparison of accuracy, MAE, and MSE, precision, recall, and F1 Score for credit card fraud detection is shown in Fig. 3 and Table 6. The accuracy, mean absolute error, mean squared error, precision, recall, and F1 Score of the ABC RNN model in comparison to the RNN model currently being used on the Credit card Dataset are all thoroughly analysed in Fig. 3. In comparison to the RNN model, which had slightly lower accuracy of 90.60 percent, higher MAE of 0.417, higher MSE of 0.330, precision of 90.81 percent, Recall of 86.12, and F1 Score of 84.31, the ABC-RNN model had improved accuracy of 97.92 percent Fig. 4, a lower MAE of 0.119, a lower MSE of 0.301, and precision of 97.93 percent, Recall of 92.25 and F1_Score of 97.16.

In Tables 7–9 shows the accuracy for different dataset. From those table, accuracy in % is increased in proposed method (ABC-RNN) when compared to the different existing methods.

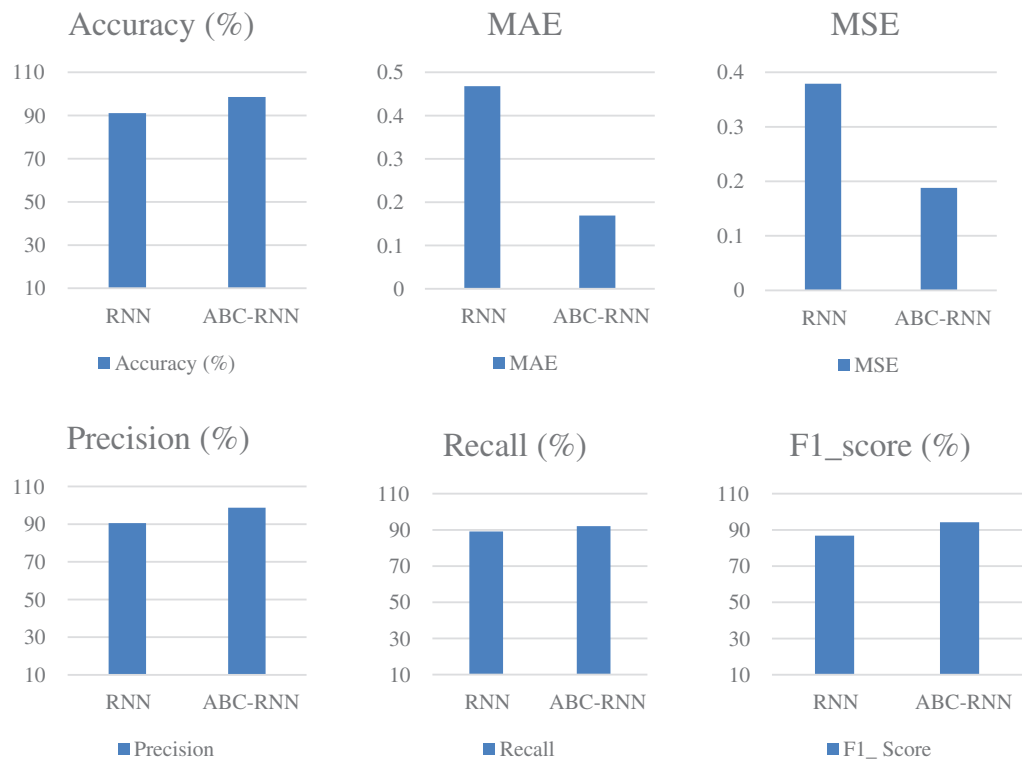

Figure 3: Comparison of performance for insurance fraud dataset

Table 6: Comparison of performance for mortgage fraud dataset

Technique	Accuracy (%)	MAE	MSE	Precision (%)	Recall (%)	F1_score (%)
RNN	90.60	0.417	0.330	90.81	86.12	84.31
ABC-RNN	97.92	0.199	0.301	97.93	92.25	97.16

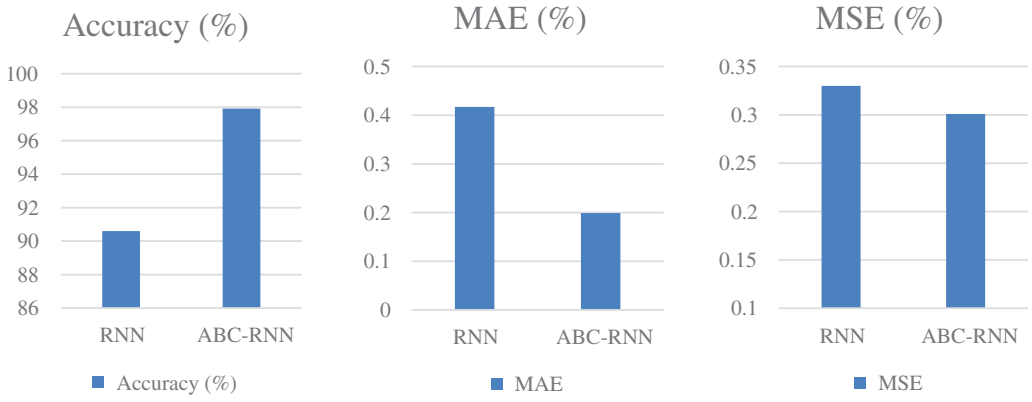

Figure 4: (Continued)

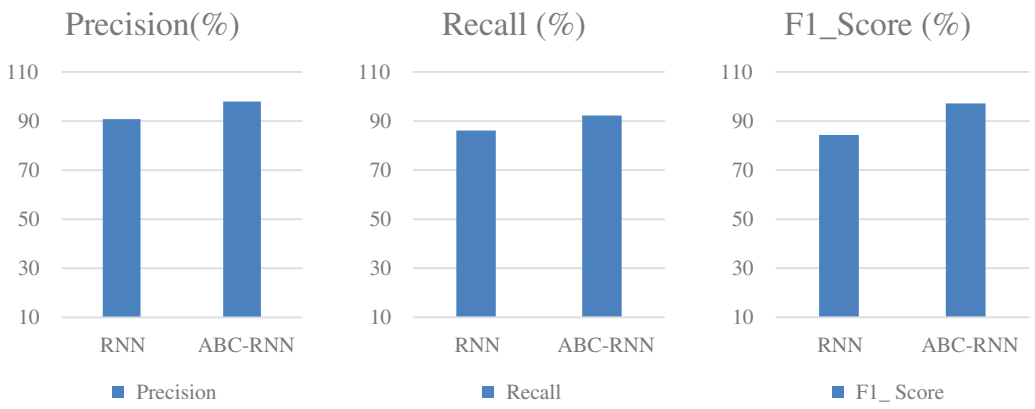

Figure 4: Comparison of performance for mortgage fraud dataset

Table 7: Comparison of performance for different approaches for credit card fraud dataset

Credit card fraud dataset		
References	Methods	Accuracy (%)
Proposed	ABC-RNN	96.03
Esraa Faisal Malik et al., (2022)	Adaboost + LGBM	82
Ajeet Singh & Anurag Jain (2021)	CFS + RF + firefly	96
Maria Nancy et al., (2020)	CNN + KNN	94

Table 8: Comparison of performance for different approaches for insurance fraud dataset

Insurance fraud dataset		
References	Methods	Accuracy (%)
Proposed	ABC-RNN	98.60
Theja et al., (2020)	CF + XGBoost	98
Yao Zhi Xu et al., (2019)	DT + LR	72
Bing Chu et al., (2018)	RF + CNN	92

Table 9: Comparison of performance for different approaches for mortgage fraud dataset

Mortgage fraud dataset		
References	Methods	Accuracy
Proposed	ABC-RNN	97.92
Bahari Belaton et al., (2022)	Adaboost + SVM	91
Nandwan. (2021)	PCA + XGBoost	93
Maoguang Wang et al., (2018)	XG-Boost + LR	83

In Tables 10–12 shows the MAE and MSE value for different dataset. From those table, errors are decreased in proposed method (ABC-RNN) when compared to the different existing methods

Table 10: Comparison of performance for different approaches for credit card fraud dataset

Credit card fraud dataset			
References	Methods	MAE	MSE
Proposed	ABC + RNN	0.205	0.360
Hasoon et al., (2022)	DNN + LSTM	0.237	0.413
Meran et al., (2020)	LSTM + NN	0.281	0.371
HAsaniuo et al., (2016)	PSO + KNN	0.224	0.780

Table 11: Comparison of performance for different approaches for insurance fraud dataset

Insurance fraud dataset			
References	Methods	MAE	MSE
Proposed	ABC + RNN	0.169	0.188
Oikonomidis et al., (2022)	CNN + XGBoost	0.263	0.374
Yan Li et al., (2019)	LSTM + CNN	0.181	0.412
Lin et al., (2017)	NN + LSTM	0.192	0.382

Table 12: Comparison of performance for different approaches for mortgage fraud dataset

Mortgage fraud dataset			
References	Methods	MAE	MSE
Proposed	ABC + RNN	0.199	0.301
Agarwal et al., (2022)	PSO + NN	0.335	0.365
Ajeet Singh et al., (2019)	SVM + RF	0.412	0.363
Anurag et al., (2019)	KNN + PCA	0.498	0.323

In Tables 13–15 shows the performance of Precision, Recall and F1_Score for different dataset. From those table, the proposed method (ABC-RNN) obtains best results when compares to the existing hybrid approaches.

Table 13: Comparison of performance for different approaches for credit card fraud dataset

Credit card fraud dataset				
References	Methods	Precision (%)	Recall (%)	F1_score (%)
Proposed	ABC + RNN	97	93	92
Esra Faisal Malik et al., (2022)	Adaboost + LGBM	96	64	77
Maria Nancy et al., (2020)	CNN + KNN	95	91	97
Shamitha and Ilango et al., (2019)	SMOTE + RF	86	82	90

Table 14: Comparison of performance for different approaches for insurance fraud dataset

Insurance fraud dataset				
References	Methods	Precision (%)	Recall (%)	F1_ score (%)
Proposed	ABC + RNN	97	93	92
Patil et al., (2021)	XGBoost + CTGAN	84	84	92
Patil et al., (2021)	Regression + CTGAN	81	81	91
Shakya et al., (2018)	SMOTE + LR	90	88	71

Table 15: Comparison of performance for different approaches for mortgage fraud dataset

Mortgage fraud dataset				
References	Methods	Precision (%)	Recall (%)	F1_ score (%)
Proposed	ABC + RNN	97	93	92
Shirodkar et al., (2022)	LR + GA	59	89	51
Abdallah et al., (2021)	CNN + LSTM	93	94	93
Shakya et al., (2018)	XGBOOST + SMOTE	53	88	66

8 Conclusion

Online transactions are essential in today's modern age of global technology because all that is required to finish an application and charge money is the user's credit card details. Therefore, it's essential to create the best strategy for identifying the most of frauds in online systems. Utilizing accuracy, MAE, MSE, Precision, Recall, and F1 Score, the effectiveness of the proposed and existing techniques is examined. The performance result shows that the suggested technique is effective and outperforms the current methods. For three data sets, the suggested method outperforms existing strategies, including RNN, in terms of accuracy. The achievement of the highest accuracy demonstrates that the suggested strategy is effective in identifying cyber-attacks. The proposed method has a lower error rate than the currently used methods. In this method we took financial fraud detection as major issues while doing online transactions. Our proposed ABC-RNN approach achieved accuracy index

as 97% and we compare the result with existing methods. May be our proposed method detects the already taken or available dataset which can be simulated by predefined set of conditions. In future we can try full automated or connected neural network for dependencies prediction.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Abdallah, M. Maarof and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, 2020.
[2] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers and Security*, vol. 57, pp. 47–66, 2019.
[3] V. Vlasselaer, V. Eliassirad, T. Akoglu and L. Snoeck, "Gotcha! network-based fraud detection for social security fraud," *Management Science*, vol. 63, no. 9, pp. 3090–3110, 2017.
[4] J. Awoyemi, O. Adetunmbi and S. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *IEEE Int. Conf. on Computing Networking and Informatics*, Singapore, pp. 1–9, 2020.
[5] S. Huang, Y. Lin, C. Chiu and D. Yen, "Fraud detection using fraud triangle risk factors," *Information Systems Frontiers*, vol. 19, no. 6, pp. 1343–1356, 2019.
[6] A. Chouiekh and J. Haj, "Convnets for fraud detection analysis," *Procedia Computer Science*, vol. 127, pp. 133–138, 2019.
[7] D. Dalpozzolo, A. Boracchi, G. Caelen and O. Alippi, "Credit card fraud detection: A realistic modeling and a novel learning strategy," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784–3797, 2017.
[8] B. Baesens, V. Vlasselaer and W. Verbeke, "Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection," *John Wiley & Sons*, vol. 27, pp. 145–185, 2019.
[9] C. Bahnsen, C. Aouada, D. Stojanovic and B. Ottersten, "Feature engineering strategies for credit card fraud detection," *Expert Systems with Applications*, vol. 51, pp. 134–142, 2019.
[10] T. Kummer and P. Best, "The effectiveness of fraud detection instruments in not-for-profit organization," *Managerial Auditing Journal*, vol. 10, no. 2, pp. 901–923, 2017.
[11] S. Majhi, "Fuzzy clustering algorithm based on modified whale optimization algorithm for automobile insurance fraud detection," *Evolutionary Intelligence*, vol. 14, no. 1, pp. 35–46, 2019.
[12] D. Cheng, S. Xiang, C. Shang and L. Zhang, "Spatio-temporal attention-based neural network for credit card fraud detection," in *AAAI Conf. on Artificial Intelligence*, Malaysia, vol. 34, no. 1, pp. 362–369, 2020.
[13] A. Zakaryazad and E. Duman, "A profit-driven artificial neural network (ANN) with applications to fraud detection and direct marketing," *Neurocomputing*, vol. 175, pp. 121–131, 2019.
[14] S. Georgieva and V. Pavlov, "Using neural network for credit card fraud detection," *AIP Conference Proceedings*, vol. 2159, no. 1, pp. 3–13, 2019.
[15] J. Jurgovsky and O. Caelen, "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2020.
[16] U. Fiore, D. Santis, A. Perla, F. Zanetti and F. Palmieri, "Using generative adversarial networks for improving classification effectiveness in credit card fraud detection," *Information Sciences*, vol. 479, pp. 448–455, 2019.
[17] A. Pumsirirat and L. Yan, "Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, pp. 18–25, 2018.

[18] S. Wang and W. Xu, "Session-based fraud detection in online e-commerce transactions using recurrent neural networks," in *European Conf. on Machine Learning and Knowledge Discovery in Databases*, China, pp. 241–252, 2019.
[19] V. Nipane, P. Kalinge, S. Vidhate and B. Deshpande, "Fraudulent detection in credit card system using SVM & decision tree," *International Journal of Scientific Development and Research*, vol. 1, no. 5, pp. 590–594, 2019.
[20] R. Cheng and Y. Jin, "A competitive swarm optimizer for large scale optimization," *IEEE Transactions on Cybernetics*, vol. 45, no. 2, pp. 191–204, 2020.