Computers and Electrical Engineering 102 (2022) 108132

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Autonomous credit card fraud detection using machine learning approach☆☆

J Femila Roseline [a,*], GBSR Naidu [b], Dr. V. Samuthira Pandi [c], S Alamelu alias Rajasree [d], Dr.N. Mageswari [e]

[a] Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India
[b] GMR Institute of Technology, RAJAM, 532127, AP, India
[c] Department of ECE, Saveetha Engineering College, Chennai, India
[d] Sri Ramakrishna Engineering College, Coimbatore, 641022, Tamil Nadu, India
[e] Ashoka Women's Engineering College, Kurnool, 518218, Andhra Pradesh

ARTICLE INFO

Keywords:
Credit card
Fraud
Machine learning
Long short-term memory-recurrent neural network
Naive Bayes
Support vector machine
Artificial neural network

ABSTRACT

Credit card fraud has risen in vulnerable effects in recent years as more people use credit cards to pay for products. This is owing to advancements in technology and growths in internet transactions, both of which have resulted in massive financial losses due to fraud. To reduce such losses, an effective fraud detection system must be designed and implemented. Machine learning approaches used to detect credit card fraud automatically and do not take into account deception process or behavioral problem, which might lead to alerts. The goal of this study is to figure out how to spot credit card fraud. To detect the occurrence of fraud, a Long Short-Term Memory-Recurrent Neural Network (LSTM-RNN) is proposed. In addition, an attention mechanism has been included to increase performance even more. In instances like fraud detection, where the information sequence is made up of vectors with complicated interrelated properties, models with this structure have proven to be particularly efficient. LSTM-RNN is compared to other classifiers such as Naive Bayes, Support Vector Machine (SVM), and Artificial Neural Network (ANN). Experiments reveal that our proposed model produces powerful results and has a high level of accuracy.

1. Introduction

Digital payments are the most prevalent payment option in recent years as a result of technological improvements and the introduction of new e-funding options alternatives, such as e-commerce and phone banking. Credit card fraudhas surged as a result of these new technologies [1]. As closer to a cashless society, online payment platforms have become increasingly vital in our daily lives. Hundreds of millions of consumers utilize the major online payment systems every dayand millions of cashless transactions are processed each day. To provide a trustworthy service, one of the most important and difficult issues is to secure the security of all

☆ This paper is for special section VSI-cps2. Reviews were processed by Guest Editor Dr. Rajesh Manoharan and recommended for publication.

* Corresponding author.
E-mail addresses: femila14@gmail.com (J. Femila Roseline), naidu.gbsr@gmrit.edu.in (G. Naidu), samuthirapandime@gmail.com (V. Samuthira Pandi), alamelurajasree.s@srec.ac.in (S. Alamelu alias Rajasree), magesmaniengg@gmail.com (Dr.N. Mageswari).

https://doi.org/10.1016/j.compeleceng.2022.108132
Received 4 December 2021; Received in revised form 19 May 2022; Accepted 26 May 2022
Available online 26 June 2022

transactions with fraud detection and prevention being a major duty [2].

Finding people who are committing credit card fraud involves a two-step process in which, first look for suspicious behavior, then analyze those behavior to see if fraud has occurred. The first half can be completed by an automated system, but the second requires human intervention. This indicates that fraud detection is a cost-sensitive problem in which an automated system that generates a large number of false fraud signals incurs a direct cost. As a result, the importance of a precise system during the first stage of fraud detection is critical [3].

Machine Learning is the most popular and frequently used technique due to its diverse applicability and cheap time commitment. Machine learning is an area of research and development concerned with techniques that enable systems to improve and get better without being pattern recognition. Numerous methods, such as data mining and machine learning algorithmic techniques, have been tried and failed to prevent fraud in credit card purchases. As a result, efficient and productive techniques that perform must also be designed [4].

The reviewing duration correlates to fraud identification in real time. The near actual intrusion detection system incorporates expertise rules based on long-term accumulations and machine learning algorithms to fire alarms on credit cards that display questionable transactions in the hours of authorized transaction. After that, experienced investigators normally review the alerts, or an automatic SMS is issued to the cardholder inviting them to verify their recent transactions and if necessary, block the card. The cardholder may be contacted to categories any transaction records in order to determine when the fraud began [5].

This paper's main objective is to assign machine learning techniques to do pattern recognition on a card transaction database and recognize suspicious transactions. The concept is to use statistical models to determine whether or not a transaction is valid. To solve the problem of class imbalance, a variety of random approaches will be used, as well as machine learning algorithms like as Naive bayes, SVM, ANN, and LSTM, which will be applied to the dataset and the results given. The important contributions of the paper are listed below.

- Develop a new credit card fraud detection system based on a recurrent neural network with a long short-term memory (LSTM-RNN)
- To effectively predict illegal service charge behaviour and to enable efficient scams.
- To conduct trials on a variety of datasets, resulting in the conclusion that our method is both competitive and alternative to existing methods.

The following is a breakdown of the paper's structure: Related works are showcased in Section 2. The suggested algorithm is illustrated in Section 3 together with the study methodology. Section 4 contains the results, as well as discussion and confirmation of the results using existing methodologies, and Section 5 depicts the conclusion.

2. Related works

Numerous techniques, including supervised, unsupervised, and hybrid algorithms, have been used to detect fraud in past studies. The types and patterns of fraud are changing all the time. It is critical to have a thorough understanding of the fraud detection technology. In this section, we'll go through the machine learning models, algorithms, and fraud detection models that have been employed in previous research. When dealing with enormous amounts of data, the author of [9] explored data mining approaches, which take time to process. Overlapping is another issue with credit card payment data preparation. To address an unequal histogram, sampling strategies are performed.

The author in [10] discussed misleading statistics, which is data that has been skewed. When compared to normal transactions, fraud transactions are quite rare. When a regular payment appears to be fraudulent or when a fraudulent transaction appears to be legal. Also, talk about the challenges of dealing with categorical data. Categorical data will be ignored by several machine learning techniques. Consider the cost of detection and adaptability as a challenge. The cost of fraud prevention and the cost of fraudulent behavior are both taken into account. The author in [11] described imbalance problem and how to deal with it, as well as how to work with enormous datasets. These obstacles were solved by the performed effort.

For detecting fraud, the author in [12] used a variety of models. Various algorithms are utilised in each concept. If fresh data exhibits substantial changes in fraud trends, detecting credit card fraud for new crimes will be difficult. It's dangerous to replace the strategy because machine learning algorithms require a long opportunity to prepare instead of forecast. The classification method is sorted using the Logistic Regression technique (LR) in [13] Fraudulent situations are distributed using Gaussian Mixture Models. Artificial group oversampling is used to equalize datasets. Economic value is calculated via scenario analysis.

This Risk Based Ensemble model is utilized in [14]. This approach can result in positive outcomes for information with problems, and the Naive Bayes technique[15,16] is used to reduce implicit noise in transactions[17]. The author in [18] narrated how a large proper date is a major concern. Real-world data is confidential and private, making it challenging to assess and execute techniques. They were assessed using both standard and actual information in [19]. An overview of the methodologies' advantages and drawbacks was reviewed. As a quality statistic, the Matthews Correlation Coefficient (MCC) [20] was chosen. To test the techniques' robustness, distortion was injected to the data.

3. Methodology

This section describes our proposed credit card fraud detection model, which is based on the LSTM-RNN architecture. This model's steps are outlined below.

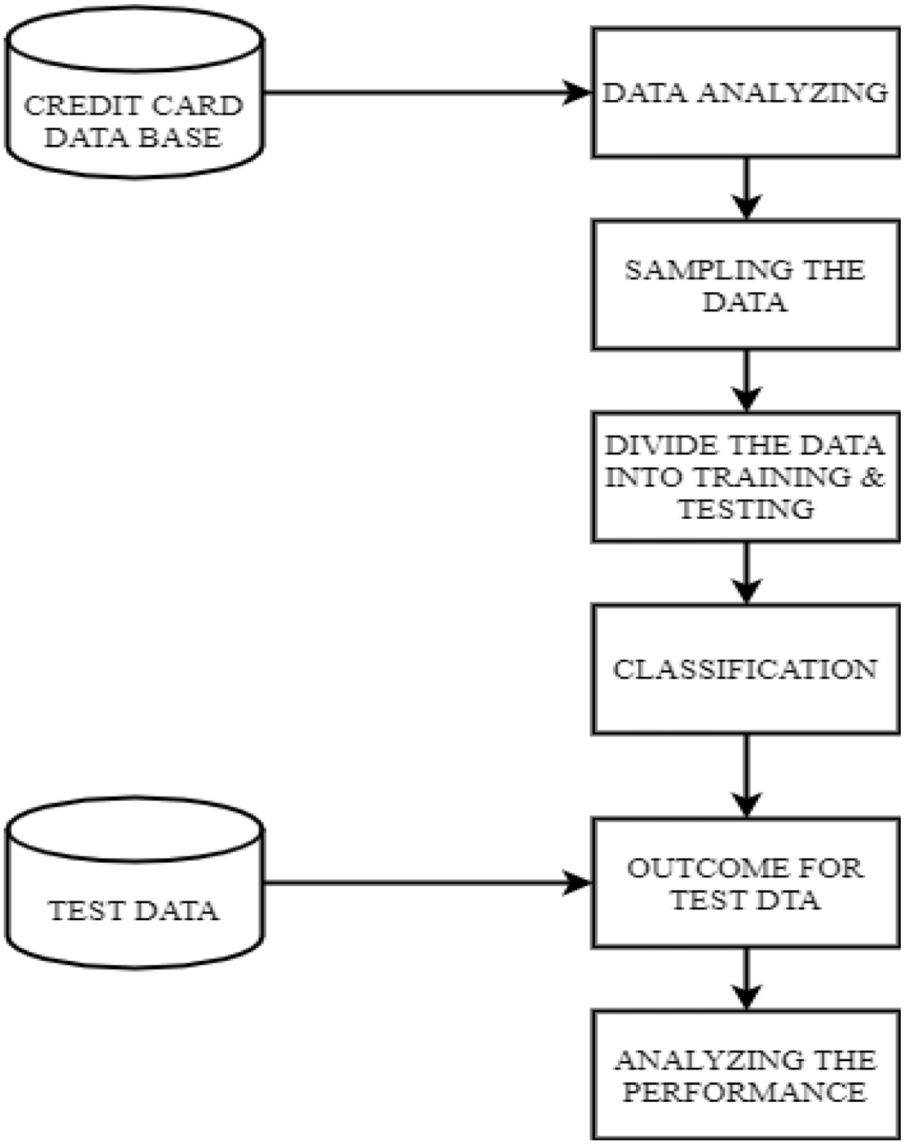

Fig. 1. Proposed methodology.

3.1. Data preprocessing

The model's accuracy is determined by the number of data used to train it. The model's performance will be improved as more data is collected. The data is cleaned and preprocessed in this initial stage as follows:

Cleaning is the process of repairing incomplete information or deleting duplicate data from a dataset [21][22]. There are records in the dataset that are duplicated, incomplete, or have null values. Cleaning is required to eliminate such documents.

3.2. Resampling technique

Because the quantity of scam in the dataset is lower to the total number of transactions, class distribution [23] in credit card transactions is imbalanced. To tackle the problem, the sampling method is applied. Over-sampling is performed on an unbalanced dataset in order to acquire two sets of distributions for study. An information point's stepwise expansion and subtraction are placed until the over-fitting limit is achieved among existent knowledge (Fig. 1).

Recurrent Neural Network

Recurrent Neural Networks are a type of Artificial Neural that is specifically supposed to show sequence information. Deep learning algorithms lack the scalability necessary to model vast amounts of time series forecasting. Recurrent neural networks allow for the construction of links among neurons co-located in the very same layer in additional to links across layers, resulting in the formation of

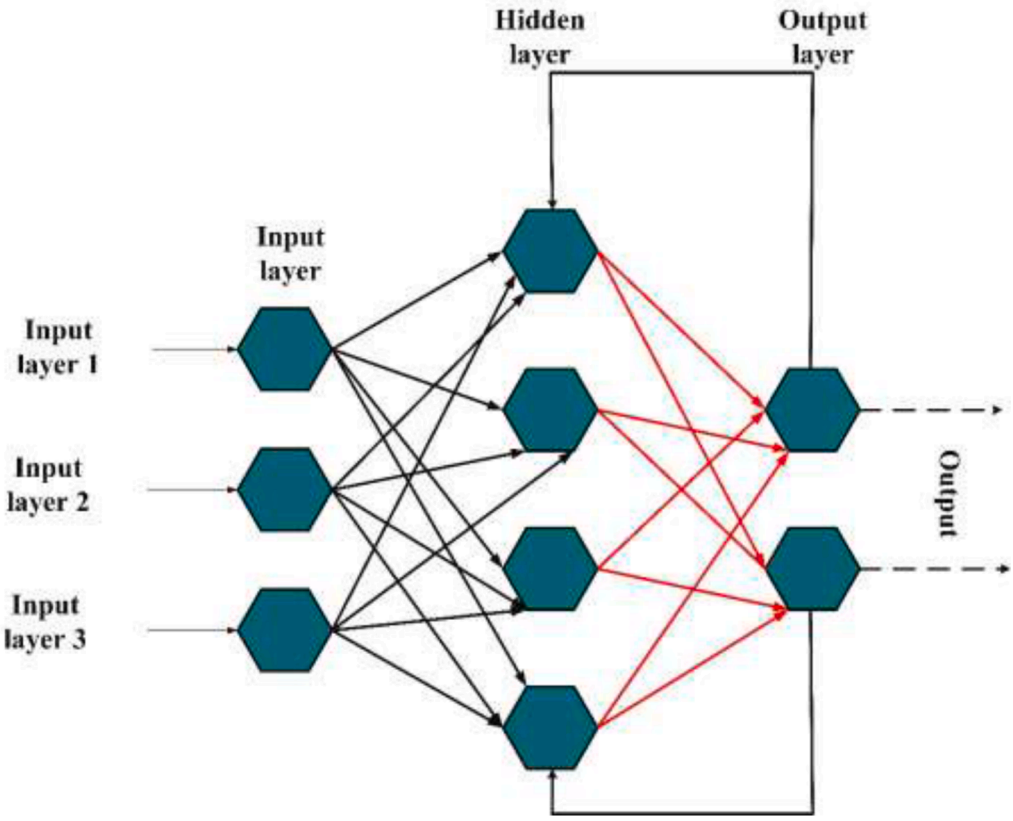

Fig. 2. Recurrent neural network with hidden layer.

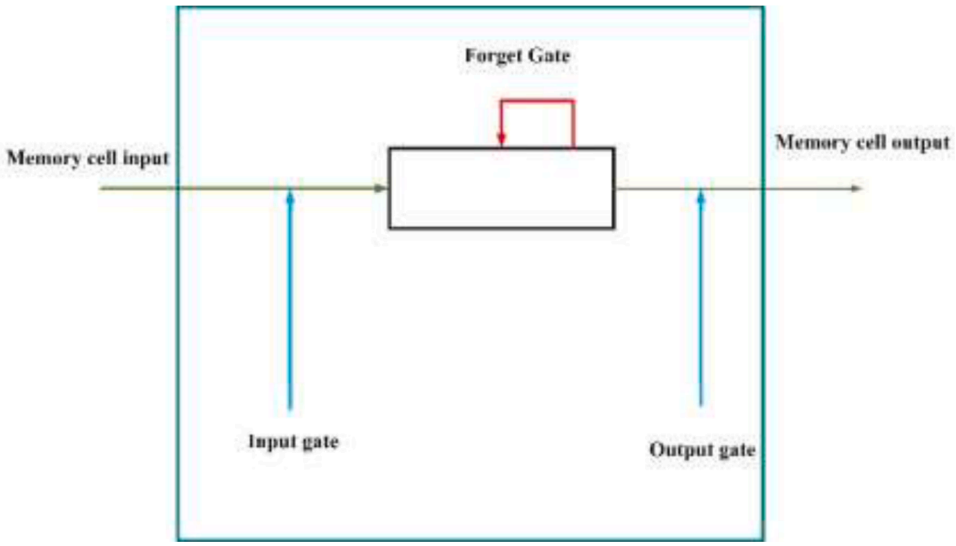

Fig. 3. Long-short term memory.

cycle in the program's architecture. Cycles allow the neurons [24,25] in the network to share weights over distinct time steps of successive values of a particular input. This allows the input layer to account for the neuron's state at an earlier point in time. As a result, the state can be used to transmit some elements of prior time periods to future time periods. The input layer, dropout rate, and loss function are all significant characteristics that influence RNN effectiveness. The Following Fig. 2 Recurrent Neural Network with Hidden layer is presented.

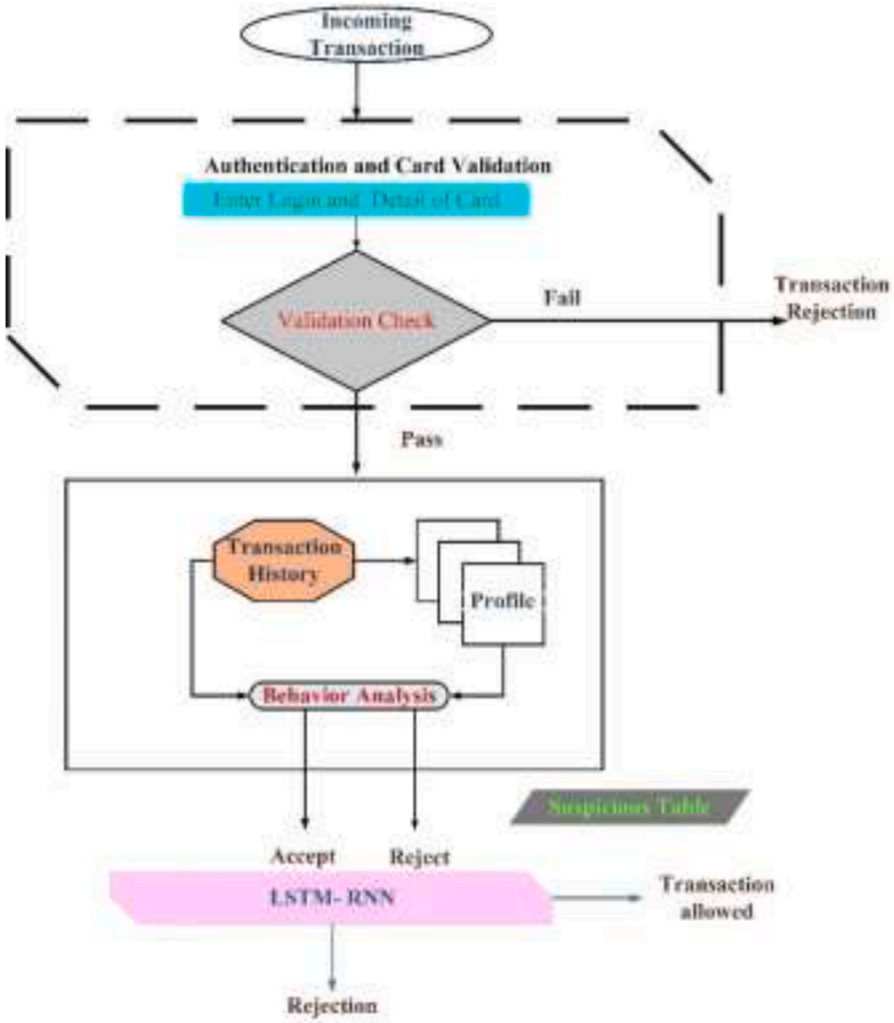

Fig. 4. Credit card fraud detection.

Long Short-term Memory

Ordinary RNNs have issues with vanishing or exploding gradients. The Long Short-term Memory design was formulated to solve these difficulties. A memory cell in an LSTM retains its state throughout time. Filtering devices are also employed to control the flow of data to and from the memory cell. An input gate, in particular, can enable or prohibit the incoming signal from adjusting the cell state (i.e., sets the input gate to zero). A base station can either allow or prevent the cell state from affecting neurons in the hidden layers. The cell can recollect or recall its prior state thanks to a forget gate (Fig. 3).

The relative value of each constituent is uncertainty reduction. The sum of neurons in the hidden layers, the training algorithm and inner transfer functions, and the pass rate are all significant LSTM factors that determine the quality of the output.

3.3. Proposed classification model

The Long Short-Term Memory (LSTM) technique is an augmentation of Recurrent Neural Networks (RNNs), that are memory-based computationally more efficient neural networks, and is used in this study to develop a deep learning intrusion detection model. It is well designed for forecasting due to previous expertise and the link among prediction outputs and previous input parameters. The LSTM design enables for long-term dependency on sequence prediction concerns to be learned. It can remember long-term patterns and is important for longer-term patterns.

The internal hidden state model is maintained by the Recurrent Neural Network (RNN) which is a class of neural network. The cyclic connection between its units is directed by the temporal behavior of the arrangement with random length. The long short-term memory is also known as the hidden Markov model extension. The modeling long-term temporal dependencies are achieved by using a non-linear transition function. By adding three gated in the RNN neuron the LSTM is extended the three layers are the forgotten gate neuron, input gate neuron, and the output gate neuron. The forget gate neuron controls the current state whether to forget or not, the

output gate neuron states the output and the input gate neuron states whether the input should be read or not. The sequence in the long-term dependencies is learned when these gates are enabled. The recurrent hidden layer is effectively proliferated with the help of these three gates and this does not affect the output. The issues or the drawback in the RNN has been overcome by the LSTM, which is an effective method when compared to RNN.

$$y_t = \gamma\left(A_s.s(t-1) + A_r R_g(t)\right) \tag{1}$$

$$ip_t = \gamma\left(A_{ips}s(t-1) + A_{ipr}R_g(t)\right) \tag{2}$$

$$fg_t = \gamma\left(A_{fgs}s(t-1) + A_{fgr}R_g(t)\right) \tag{3}$$

$$op_t = \gamma\left(A_{ops}s(t-1) + A_{opr}R_g(t)\right) \tag{4}$$

$$s(t) = fg_t \odot r(t-1) + ip_t \odot y_t \tag{5}$$

$$op(t) = s(t) \odot op(t) \tag{6}$$

In the above equation "*fg*" denotes the forget gate, "*ip*" denotes the input gate and "*op*" denotes the output gate. The γdenotes the activation function and the ⊙ denotes the product of the gate value and *R* denotes the parameter of the matrices. Three neuron gates are connected to the op(t) and s(t). Each LSTM consist of an update term, input gate, forget gate, and output gate. Every gate is interconnected to each other.

In this article, we used long short-term memory networks to model the sequential dependency between credit card transactions. The hidden state design of the LSTM allows for the establishment of connections between neural network nodes over time steps.

As a result, the model may be able to store data from prior inputs, allowing it to discover temporal correlations between events that are distributed over the input sequence. The LSTM is a suitable model for succession patterns in sequential data points where the occurrence of one event may be influenced by the presence of many other occurrences in the past.

Credit Card Fraudulent

The fundamental obstacle in this topic is that the frequency of plaguing is relatively low, necessitating the detection of a rare occurrence among a huge number of valid transactions. As a result, false alerts are generated, which must be reduced. While a company's failure to discover a fraud case result in a direct loss, the follow-up activities necessary to advance the false alarms are equally costly. Our goal in this project is to not only detect credit card fraud use, but also to lower the false alert rate. The following Fig. 4 shows how the fraudulent card is detected.

Pairing the sequence doesn't really entail that the payment must exactly match the pattern; rather, the neural net determines how close the transaction is to the sequence; if there is a slight difference, the transaction is fine; if there is a significant difference, the likelihood of the transaction being illegal increases, and the neural network declares the transaction a fault transaction. The neural network is programmed to provide results in the range of 0 to 1. If the neural network generates an output that is less than or equal to 0.6 or 0.7 the transaction is lawful, but if the output is more than or equal to 0.7, the likelihood of the transaction being illegal increases.

If a legal user is unable to transact due to these restrictions, there is little cause for concern. However, when an unauthorized person obtains a credit card, he will not use it repeatedly to make a series of small transactions, but rather will attempt to make as large an acquisition as possible.

3.4. Performance metrics

The experiments are computed using four basic metrics: TPR, TNR, FPR, and FNR rates measures.

TP (True Positive): The truly positive predicts the share of suspicious transactions that were categorized as one and the same.

$$\text{Truepositive} = \text{TP}/\text{TP} + \text{FN} \tag{7}$$

True Negative (TN): The true negative prediction the share of regular transactions that is appropriately characterised as being such.

$$\text{Truenegative} = \text{TN}/\text{TN} + \text{FP} \tag{8}$$

False Positive (FP): The false-positive rate indicates the bit of the non-fake exchanges wrongly delegated as fraudulent transactions.

$$\text{Falsepositive} = \text{FP}/\text{FP} + \text{TN} \tag{9}$$

False Positive (FP): The false-positive rate is the percentage of non-fake exchanges that are mistakenly classified as fraudulent transactions.

$$\text{Falsenegative} = \text{FN}/\text{FN} + \text{TP} \tag{10}$$

4. Results and discussion

Based on the application of LSTM cells, the model efficiently and effectively predicts the credit card fraud. There are numerous

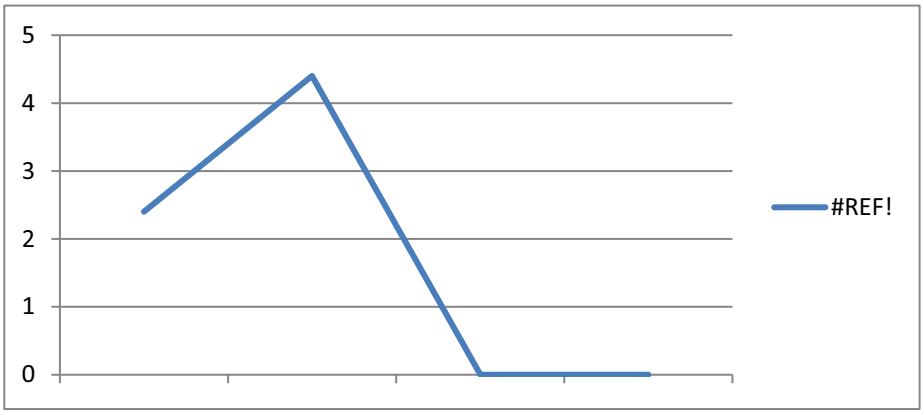

Fig. 5. ROC curve.

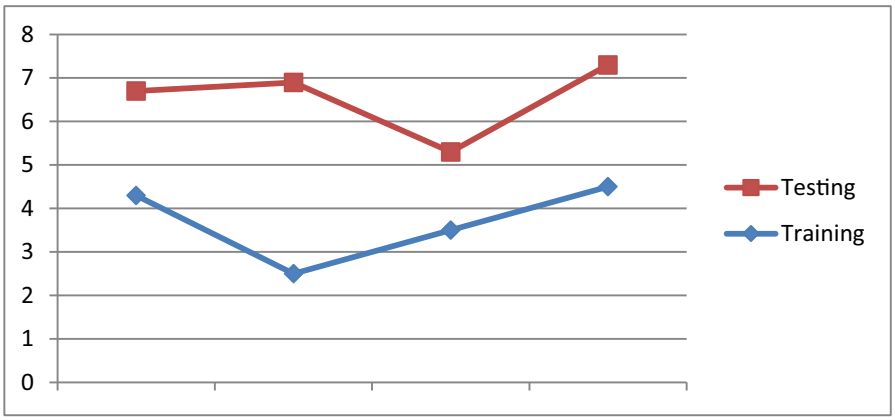

Fig. 6. Detection of credit card.

optimizers that can be utilized in this model, the proposed optimizer improves the outcomes significantly. The number of layers and iterations did not make a significant impact in the results. In addition, the results show that the number of iterations and layers have an impact on time. The findings revealed that accuracy and the number of iterations had a strong relationship.

A. Dataset

The dataset is available as a Kaggle source. This dataset describes transactions conducted over the course of two days and includes a total of 284,87 transactions. In the positive class, the dataset is uneven and skewed. The input variables are only available in numerical form because the PCA yielded these values. As a result, thirty input attributes have been implemented. Because there are some personal issues, the details and background information about the characteristics are not defined. The time attribute includes the first transaction in the dataset, as well as the seconds that elapsed between each transaction. The payment's amount is represented by the amount attribute. The factors leading is a binary classifier endpoint class that yields 1 in the positive argument and 0 in the non-fraud case.

B. Experimental Setup

The model setup is done in this section to provide persuasive proof that the LSTM model is useful in detecting abnormalities in the finance domain. The different tasks, including as pre-processing and model selection, are programmed using functions from the Python Sklearn package. The LSTM model is implemented using the Keras package (Fig. 5).

The goal is to assess the accuracy, loss rates, and time to detect credit card fraud. It also demonstrates that the LSTM model can detect both known and undiscovered fraud behavior. When watching blips on a radar screen, the ROC curve was first utilized in the Detection Algorithms Theory field as an indicator of a radar carrier's ability to differentiate between noise, friendly ships, and enemy ships. The ROC curve made its way into science and medicine in the 1970s, where it was discovered to be effective for evaluating medical test findings. It was just a matter of time until it made its way into the machine learning industry, thanks to its effectiveness in representing binary classification efficiency.

C. State of Art

These models accept input information requests, evaluate it, interpret it, and then return the results. It's the process of retrieving and responds to requests for input data. The optimization techniques figure out and understand from the facts, and the features can be

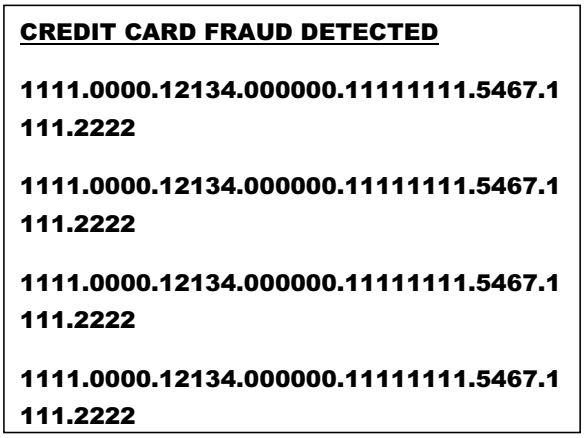

Fig. 7. Validation accuracy.

Table 1
Comparison of fraud detection.

Technique	Dataset	Preprocessing	Performance	Result
Bayesian Network Classifier	Pag Seguro	*	Precision, Recall and Economic Efficiency are between HM	Fraud BNC and this include the probability threshold and other beneficial cause such as Decision Tree
Scatter search and Genetic Algorithm	Major bank of Turkey	*	Misclassification cost and that could be based on the TP, FP, TN, FN	Existing performance is improved by 150%
Hidden Markov Model	NA	*	TP, FP	82% accuracy
Artificial Neural network, Bayesian Belief	Provided by Serge waterschool	*	TP, NP	It is noted that the Bayesian Belief is better than Artificial Neural Network
Bagging Ensemble	Real world credit card	*	False Alarm Rate, Fraud Catching and Balanced Classification	Rate of fraud catching is high and stable.

trained over a set of data. The best performing models are identified from the presented findings based on their low rate of error.SVM is used to classify and predict data for fraud detection. There has been a lot of research on detecting credit card fraud. To detect the fraud, they use the customer's prior behavior pattern. The model is built using the transaction history of a single credit card [6]. ANN predicts the credit card fraud in [7] but it is hardware dependence. The naive bayes classifier is a probability-based classifier for detecting credit card fraud. In the probability-based classification strategy, the target classes' probabilities and the test data's probabilities are computed. [8] (Fig. 6 and 7).

The following Table 1 shows the Comparison of Fraud detection approach in detail manner. outlines some of the most important machine learning-based fraud detection technologies. When precision, recall, and economic efficiency are taken into account, the Fraud Based On Bayesian Classifier followed by probability threshold outperforms Nave Bayes, Tree Supplemented Nave Bayes, Support Vector Machine (svm, and Decision Trees on the PagSeguro dataset. When combined with Dempster-Shafer Theory, Bayes Learning produced 98 percent True Positives and less than 10% False Positives. When applied to the existing systems of a big Turkish bank, Genetic Algorithms and Scatter Search boost performance by 150 %.

D. Performance Measures

Following the phase of model training, a test dataset trained model evaluates the performance of new data. The model's performance is analyzed by taking into account some significant metrics.

(i) Accuracy – The total number of correct detections over the total number of test samples. This metric can be mathematically expressed through the following equation –

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{11}$$

(ii) Error –It is the difference between the actual output and the classified output and is mathematically expressed as

$$Error = 1 - -Accuracy \tag{12}$$

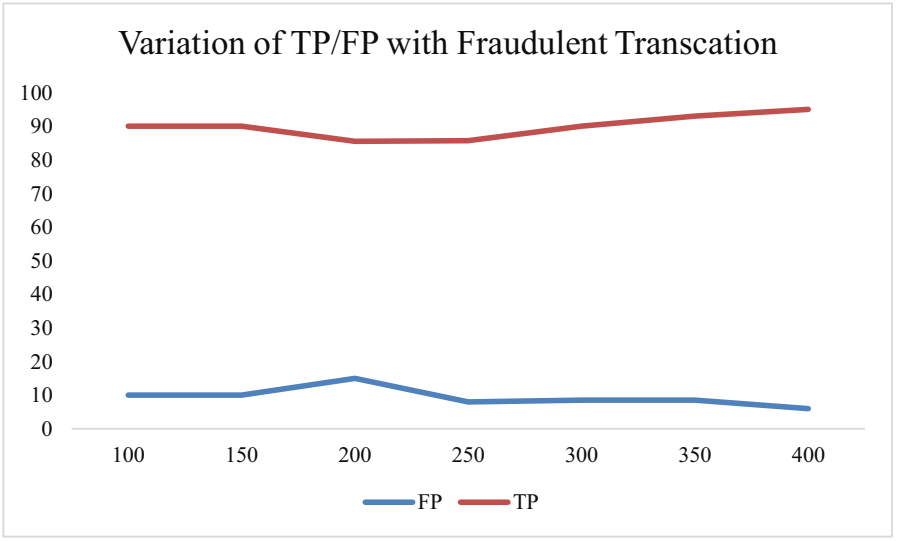

Fig. 8. Variation of TP/FP with Fraudulent Transaction.

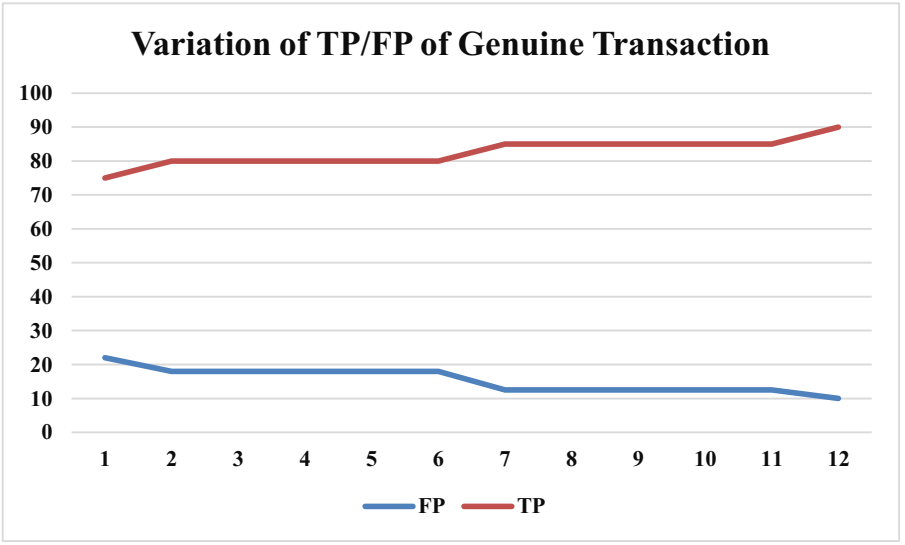

Fig. 9. Variation of TP/FP with genuine Transaction.

(iii) Sensitivity – Total number of correctly predicted positives in a set of actual positive class test samples

$$Sensitivity = \frac{TP}{TP + FN} \tag{13}$$

(iv) Precision – Total number of actual positive cases out of the predicted positives. The below given equation represents precision mathematically

$$Precision = \frac{TP}{TP + FP} \tag{14}$$

(v) Recall - Total number of correctly predicted positives out of actual positive cases. The below given equation represents recall mathematically

Table 2
Performance based on confusion matrix.

Algorithm	Precision	Recall	F-measure	Sensitivity	Accuracy
Naive Bayes	0.716	0.695	0.689	0.796	69.538%
SVM	0.688	0.666	0.656	0.64	86.56%
ANN	0.926	0.718	0.716	0.796	91.848%
LSTM-RNN	1	1	1	1	100%

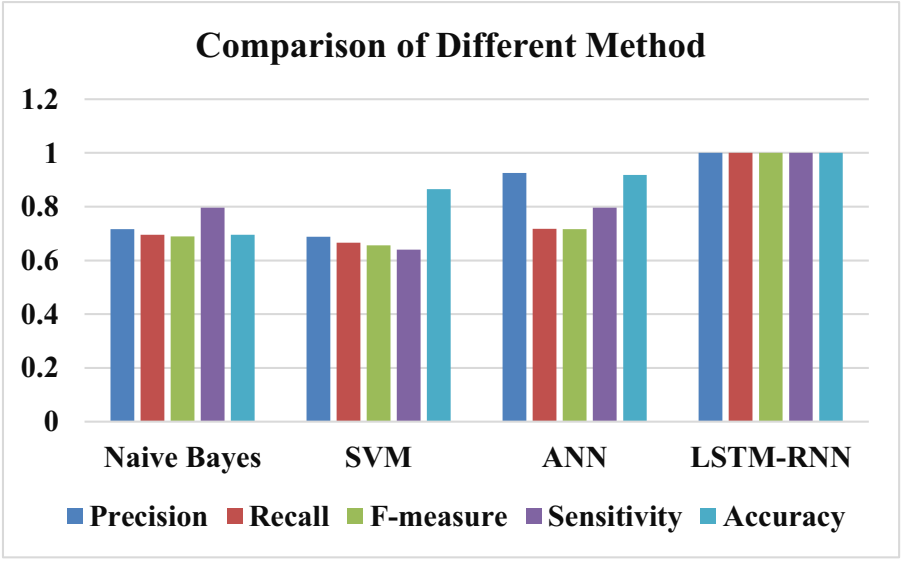

Fig. 10. Comparison of different method.

$$Recall = \frac{TP}{TP + FN} \tag{15}$$

(vi) F1- Score – Solves the trade-off between precision and recall and is mathematically expressed as weighted mean of precision, recall of the test.

$$F1 - Score = \frac{2 * Precision * Recall}{Precision + Recall} \tag{16}$$

The above Fig. 8 and 9 show the graph of variation of TP and FP based on Fraudulent and Genuine Transaction. The graph in Fig. 8 shows that as the size of genuine transactions grows, the percentage of FP reduces over time, indicating that the user's behavior is being caught more consistently. As a result, the TP rate rises as well. Similarly, Fig. 9 illustrates that as the number of fraudulent transactions (size) increases, the TP rate rises but the FP rate falls.

The confusion matrix as shown in Table 2 indicates not only the performance of a predictive model, but also which classes are correctly forecasted, which are incorrectly forecasted, and what types of errors are created. The simplest confusion matrix is for a two-class classification problem with negative and positive classes as shown in Fig. 10.

5. Conclusion

The proposed study depicted on Machine Learning models such as Naive bayes, SVM, ANN, and LSTM-RNN which have been utilized to detect fraud in the credit card system. The suggested system's performance is measured using sensitivity, precision, accuracy, and error rate. Traditional techniques are no longer effective in the age of big data. As a result, the team developed a model for detecting credit card fraud based on the Long Short-Term Memory technique using an actual data set of credit card fraud. This model was created to improve current detection tactics as well as detection accuracy in light of big data. It used deep learning techniques to quickly and effectively identify patterns, overcoming the difficulty of recognizing unexpected and sophisticated fraud practices. The problem of inefficiency of prior solutions was also solved using the proposed model based on the LSTM technique. The outcome of the

LSTM-RNN classifier with boosting strategy outperformed the ANN, SVM and Naive bayes methods when all three methods were compared for better prediction results.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Benchaji I, Douzi S, El Ouahidi B. Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks. Journal of Advances in Information Technology 2021;12(2).
[2] Li, L., Liu, Z., Chen, C., Zhang, Y. L., Zhou, J., & Li, X. (2019). A Time Attention based Fraud Transaction Detection Framework. *arXiv preprint arXiv:1912.11760*.
[3] Nordling, C. (2020). Anomaly Detection in Credit Card Transactions using Autoencoders.
[4] Asha RB, KR SK. Credit card fraud detection using artificial neural network. Global Transitions Proceedings 2021;2(1):35–41.
[5] Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997, July). Credit card fraud detection using meta-learning: Issues and initial results. In *AAAI-97 Workshop on Fraud Detection and Risk Management* (pp. 83-90).
[6] Gyamfi NK, Abdulai JD. Bank fraud detection using support vector machine. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE; 2018. p. 37–41.
[7] Asha RB, KR SK. Credit card fraud detection using artificial neural network. Global Transitions Proceedings 2021;2(1):35–41.
[8] Mishra, A. (2021). Fraud Detection: A Study of AdaBoost Classifier and K-Means Clustering. *Available at SSRN 3789879*.
[9] Xuan GLiu, Li Z, Zheng L, Wang S, Surname GN. Random forest for credit card fraud detection. In: IEEE 15th International Conference on Networking, Sensing and Control (ICNSC); 2018.
[10] Satvik Vats, Surya Kant Dubey, Naveen Kumar Pandey, A Tool for Effective Detection of Fraud in Credit Card System, published in International Journal of Communication Network Security ISSN: 2231 1882, Volume-2, Issue-1, 2013.
[11] Rinky D. Patel and Dheeraj Kumar Singh, Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm, published by International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
[12] Hamdi Ozcelik M, Duman Ekrem. Mine Isik, Tugba Cevik, Improving a credit card fraud detection system using genetic algorithm. In: published by International conference on Networking and information technology; 2010.
[13] Wen-Fang YU, Wang Na. Research on Credit Card Fraud Detection Model Based on Distance Sum. In: published by IEEE International Joint Conference on Artificial Intelligence; 2009.
[14] Prodromidis Andreas L, Stolfo; Salvatore J. Agent-Based Distributed Learning Applied to Fraud Detection. Department of Computer Science- Columbia University; 2000.
[15] Stolfo Salvatore J, Fan Wei, Lee Wenke, Prodromidis; Andreas L. Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project"; 0-7695-0490-6/99. IEEE; 1999.
[16] Soltani N, Akbari MK, SargolzaeiJavan M. A new user-based model for credit card fraud detection based on artificial immune system. In: Artificial Intelligence and Signal Processing (AISP), 2012 16th CSI International Symposium on. IEEE; 2012. p. 029–33.
[17] Pozzolo AD, Boracchi G, Caelen O, Alippi C, Bontempi G. Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems August 2018;29(8):3784–97.
[18] Abdallah A, Maarof AM, Zainal A. Fraud detection system: A survey. J Netw Comput Appl June 2016;68:90–113.
[19] Dhok SS, Bamnote GR. Credit card fraud detection using hidden Markov model. International Journal of Advanced Research in Computer Science 2012;3(3):816–20.
[20] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," arXiv: 1009.6119, 2010.
[21] Pun J, Lawryshyn Y. Improving credit card fraud detection using a meta-classification strategy. International Journal of Computer Applications October 2012;56(10):41–6.
[22] Zhao X, Zhang J, Qin X. Loma: A local outlier mining algorithm based on attribute relevance analysis. Expert Syst Appl October 2017;84(30):272–80.
[23] Vlasselaer VV, Bravo C, Caelen O, Eliassi-Rad T, Akoglu L, Snoeck M, Baesens B. APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. Decision Support Systems July 2015;75:38–48.
[24] Ganji VR, Mannem SNR. Credit card fraud detection using anti-k nearest neighbor algorithm. International Journal on Computer Science and Engineering June 2012;4(6):1035–9.
[25] Bhatla TP, Prabhu V, Dua A. Understanding credit card frauds. Cards Business Review June 2003:1–15.

Femila Roseline J working as Associate Professor in the Department of Electronics and Communication Engineering at Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences. Her research interests include CNN and AI.

GBSR Naidu working as Senior Asst. Professor at GMR Institute of Technology .His is research interests include Artificial intelligence and Machine Learning Algorithms

V Samuthira Pandi working as Associate Professor in the Department of ECE at Saveetha Engineering College. The research interest includes Machine Learning and Deep Learning Algorithms

Alamelu alias Rajasree S is presently working as Assistant Professor at Sri Ramakrishna engineering college, Coimbatore.

N Mageswari is working as Associate Professor at Ashoka Women's Engineering College, Kurnool. Her research areas are Convolutional Neural networks and Artificial Intelligence