

Prevention of credit card fraud transaction using GA feature selection for web-based application

Kavuri Sreekanth¹, Ratnababu Mamidi², Thumu Srinivas Reddy³, Kuruva Maddileti⁴,
Darivemula Deepthi⁵

¹Department of Computer Science and Engineering, Koneru Lakshmaiah University, Guntur, India

²Department of Electronics and Communication Engineering, St. Ann's College of Engineering and Technology, Guntur, India

³Department of Electronics and Communication Engineering, Malla Reddy Engineering College, Main Campus, Dhulapally, India

⁴Department of Mathematics, KV Subba Reddy Engineering College, Kurnool, India

⁵Department of Computer Science and Business Systems, Rayapati Venkata Rangarao and Jagarlamudi Chandramouli College of Engineering, Guntur, India

Article Info

Article history:

Received Jan 11, 2024

Revised Apr 19, 2024

Accepted May 7, 2024

Keywords:

Credit card fraud

Feature selection

Fraud detection

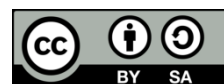
Genetic algorithm

Prevention

ABSTRACT

Credit card fraud (CCF) is a regular event that generates financial losses. A considerable share of the significantly increased volume of internet transactions is made with credit cards. CCF detection programmes are consequently highly prioritised by banks and other financial organisations. These fraudulent transactions can come in a wide variety of formats and categories. To maintain data integrity, financial institutions support digital transactions. One of the most popular ways to pay the products and services can be done by both online and offline by using a credit card. Thus, there is a higher possibility of fraud during these financial transactions. This informs programmers to the requirement for a reliable technique for identifying successful fraud. Credit card users and businesses that accept credit cards have recently had to contend with the serious issue of CCF. Application-level frauds and transaction level frauds are the two categories into which CCF controlled frauds are divided. Therefore, utilizing genetic algorithm (GA) feature selection for web-based applications, it is advised to use this strategy as a method for the prevention of CCF transaction. This method's performance is evaluated based on a number of factors, including accuracy, recall, and specificity.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Kavuri Sreekanth

Department of Computer Science and Engineering, Koneru Lakshmaiah University

Guntur, Andhra Pradesh, India

Email: kavurikanth@gmail.com

1. INTRODUCTION

Credit card fraud (CCF) is a significant problem that has negative effects on businesses, financial institutions, and regular people. The development of contemporary technology over the past 20 years, particularly the internet and portable computers, has led to a surge in financial fraud [1]. For example, an account holder's credit card information could be stolen by a criminal who would then use it to carry out fraudulent transactions. The activities may have an impact on how illegal organisations, like organizations that transport drugs and terrorists, manage their income [2].

Due to the complexity of the problem, traditional solutions that depend on manual methods, such as auditing, come up short of meeting the needs of modern life while still ensuring that credit card payments are secure. However, machine learning techniques have proven to be helpful because of their capacity to find little irregularities in huge databases. According to our explanations, fraud can be perfectly described as the

determined use of criminal methods to profit financially [3]. Nowadays, the fact that finance is an essential part of life because fraud detection in banking is one of the most important aspects. In order to enhance the analytical server's performance in constructing models and keep up with the increasing amount of data in peta bytes, in order to read data quickly and send it to the analytical server for fraud prediction, an analytical framework has been integrated with Hadoop [4].

The banking information system has considerably increased the efficiency and profitability of both the public and commercial sectors. Credit cards are widely utilized as a form of payment because of the increase in e-commerce, internet technology, online banking, and improvements in mobile smart devices. This is especially true for online business transactions made using web payment gateways such as PayPal, Alipay, and others. CCF is growing quickly as credit card transactions overtake cash as the main form of payment for both online and offline transactions [5].

Digital or physical credit card transactions both are available. Credit card numbers are typically swiped or scanned by a device while making physical transactions; however, cardholders usually provide their card number, expiration date, and card verification number over the phone or online when making digital payments. The several permission processes in place aren't effective in blocking, according to CCF [6]. Fraud detection and fraud prevention are two techniques that are regularly used to stop thieves from stealing money [7]. Fraud detection includes monitoring cardholder transaction behavior to determine if an incoming transaction is being performed by the cardholder or by criminals. Fraud prevention stops fraudulent transactions in their tracks even if it's a defensive measure. To begin with, a lot of people utilized data mining techniques to identify fraudulent transactions using traditional methods, which is not usual because modern fraudsters are so smart that they may commit fraud without exceeding any regulations [8]. Thus, it is conventional to use machine learning. Unauthorized use of a credit card account without the owner's knowledge is known as a fraudulent credit card transaction. In order to prevent similar situations in future transactions, preventative measures against such fraudulent behaviors must be implemented by analyzing and evaluating these fraud transactions [9].

Anomaly detection and misuse detection are the two types of fraud detection. Classification techniques are used in fraud detection to evaluate whether an incoming transaction is fraudulent. This technique often uses a pattern to discover different fraud schemes that are already in operation. Anomaly detection creates a historical transaction pattern for the behavioural profile of a cardholder's typical transaction when an incoming transaction deviates from the regular transaction pattern and evaluates if it is probably fraudulent [10].

Fraud in financial transactions is identified by classifying a transaction involving a user as an outlier because it deviates from usual user behaviour. To increase the value of the business, the detection process is frequently done in real-time when it comes to online transactions [11]. Once an application has been generated, frauds are discovered by analyzing the transaction data, which is frequently kept on an operational data store. Post-adjudication fraud identification typically has a significantly negative effect on the company's valuation because of the cost of collection, the significance threshold of the amount involved, and the probability of successful collection [12].

By examining past fraud trends, banking institutions can spot fraudulent behaviour and take immediate corrective action. Any fraud detection system used nowadays must be web-based due to advantages such as WS-I, which creates a more simple channel for data exchange between different applications. Statelessness, discoverability, reusability, composability, and independence are more features it offers. This method describes a strategy for developing an online fraud detection model and determining the validity of a transaction. Obtaining credit card transaction datasets that are highly imbalanced, choosing the optimal features for the models, and implementing the right performance assessment metrics are some of the difficulties in credit card detection. These issues are crucial in order to stop the misuse of CCF data. Determining the detection rate at which the model can classify involves work, and the goal in the end is to determine the fraudulent transactions that can be identified using credit card information [13].

Based on two levels of evaluation, 66 machine learning models are analyzed in this paper. All models use stratified K-fold cross-validation and a real-world dataset of European cardholders for CCF detection. Nine machine learning methods have been implemented in order to identify fraudulent transactions in the first round. Nineteen resampling strategies are used with top three algorithms. The best suggested model is thought to be the All K-nearest neighbors (AllKNN) undersampling technique combined with CatBoost (AllKNN-CatBoost) out of 330 evaluation metric values that took about a month to achieve. Consequently, a comparison is made between the AllKNN-CatBoost model and related works [14].

Using a real card transaction data set, a hybrid data mining/complex network classification technique is given that may identify instances of illegal activities. Its foundation is a newly suggested network reconstruction approach that makes it possible to show exactly one instance differs from a reference group. In operation, we demonstrate how the integration of features extracted from the network data

representation enhances the resulting score of a standard neural network-based classification algorithm and furthermore how this combined approach can outperform a commercial fraud detection system [15].

ML algorithms are used to identify CCF. First, common methods are applied. There is use of hybrid strategies such as majority voting and Adaboost. A dataset that is available to the public is used to evaluate the model's efficiency. The real world-dataset is analyzed. The results indicated that majority voting technique achieved better accuracy for CCFs detection [16].

A deep learning algorithm is described that contains a gated recurrent unit (GRU) and long short-term memory (LSTM) as base learners in an ensemble algorithm with multi-layer perceptron (MLP) as a meta-learner. Hybrid oversampling method is edited nearest neighbour technique is used for dataset class distribution balance. Improved results in terms of specificity and accuracy were obtained with this method [17].

The light gradient boosting machine (LightGBM) parameters are intelligently controlled by the intelligent integration of a hyper parameter optimization technique based on Bayesian analysis. Experiments are performed using two publicly available credit card datasets which contains legitimate and fraudulent transaction images to determine the effectiveness of presented technique for fraud detection of credit cards. This system achieved 92% accuracy and 56.95% f1-score [18].

First a ML technique is applied to the dataset to improve the detection technique accuracy. Next three frameworks based on convolutional neural network (CNN) is applied for improving detection performance. The result analysis is performed while applying different combinations of hidden layer, epochs. The results shows that this technique has obtained good results in terms of accuracy, precision, F1-score and area under the curve (AUC) [19].

The fraud detection problem formalization is described which demonstrates the real conditions of fraud detection systems which analyze the huge amounts of credit card transactions daily. Appropriate performance measures also described to evaluate the performance. A new strategy is described and it addresses the class imbalance, drift concept and verification latency. Finally, the result analysis declared that the class imbalance and drift concepts have significant impact on credit card transactions. In addition, it is observed that, if the impact is less then precise alerts will be less [20].

Using a hybrid data sampling strategy in combination with an ensemble neural network algorithm, an effective method for detecting CCF is presented. The ensemble algorithm is obtained through LSTM as a base learner in Adaboost method. Two publicly available dataset are used to measure the performance. The obtained results indicate that this approach is performed effectively when it is trained with re-sampled data [21].

A presentation on machine learning for CCF detection is given. The primary goal of this research is to detect CCF detection using machine learning methods. The Adaboost algorithm and the random forest algorithm are the ones that are utilized. The accuracy, precision, recall, and F1-score of the two algorithms are used to compare their results. The confusion matrix is used to plot the ROC curve. When the random forest and Adaboost methods are compared, the approach with the highest recall, accuracy, precision, and F1-score is considered to be the most effective one for fraud detection [22].

The paper describes predictive modeling for data analytics-based CCF detection. In order to detect frauds on a real-time basis and provide minimal risk and high customer satisfaction, a big data analytical framework is used to process huge amounts of data. Various machine learning algorithms are utilized for fraud detection, and their performance is monitored on benchmark datasets [23].

It describes transaction behavior-based CCF detection. In the event that the system fails, this study suggests having a detection model available to identify potentially unusual transactions. When the model was being created, a number of classifiers were evaluated; however, only the random tree and J48 produced the greatest accuracy scores. A further examination of these two classifiers reveals that the J48 matches the transaction log data better [24].

Using an ensemble model, a framework for predictive analytics as a service is described. The ensemble model that forms the basis of the framework that is being described makes use of the most effective prediction algorithms, including gaussian process (GP), auto regression algorithm (ARX), and artificial neural networks (ANN). The first prediction algorithm, ANN, is evaluated on sample dataset and predictive analytics as a service framework is described [25].

Machine learning algorithms for CCF detection is provided. Using traditional machine learning algorithms, statistics, calculus (dierentiation and chain rule), and linear algebra to build complex machine learning models for prediction and data set understanding, the project's goal is to predict fraud and fraud-less transactions with respect to the time and amount of the transaction. When this method is tested for accuracy, decision trees, ANNs, and logistic regression provide results that are more accurate than those of any other algorithm [26].

A novel oversampling technique is presented and it generates diverse and convincing minority class data. The generated minority data is used to improve the training performance in order to train the ensemble classifier. This technique is tested over an open credit card dataset. The oversampling technique with varaitional autoencoder generative adversarial network (VAE-GAN) is used to improve the accuracy.

Compared to other algorithms, presented technique with VAEGAN shown good results in terms of F1-score and precision. This approach deals with imbalanced data problem [27].

By combining an improved support vector machine (SVM) with a quantum solver, a detection framework is created and implemented into practice utilizing quantum machine learning (QML). Different ML algorithms are implemented to evaluate the performance on two datasets namely time series (bank loan dataset) and non-time series dataset (Israel credit card transactions). QML performance is compared with ML algorithms. The results indicate that quantum enhanced SVM has high speed and accuracy for time series dataset [28].

To solve the above-mentioned issues, prevention of CCF transaction utilising genetic algorithm (GA) feature selection for web-based application is presented. The following describes the way the paper is organized: After the introduction, the literature review is presented. The suggested methodology is presented in section 2. The analysis of the results is evaluated in section 3. The conclusion marks the end of section 4.

2. PREVENTION OF CCF TRANSACTION USING GA FEATURE SELECTION FOR WEB BASED APPLICATION

In this section prevention of CCF transaction utilising GA feature selection for web-based application is presented. The block diagram of proposed methodology is shown in Figure 1. The University of California, Irvine (UCI) repository is the initial source of the dataset used in this methodology. Our learning used the German credit dataset to classify the transactions as real or fraudulent. Only a portion of the dataset from the UCI repository is accessible. 1,000 instances (credit candidates) and 21 attributes (14 definite/insignificant and 7 numerical) are included in the dataset. Access in the dataset refers to a person who receives credit from a bank, with each occurrence representing a specific member's credit standing, whether good or negative. Based on a specific set of characteristics, every person is categorised as having excellent credit or bad credit. Second, duplication in the dataset was eliminated through pre-processing of the data. By reducing duplicated features in the dataset, the feature selection (FS) strategy enhances learning performance. The FS process increases the accuracy of fraud detection and reduces the influence of irrelevant factors on CCFs.

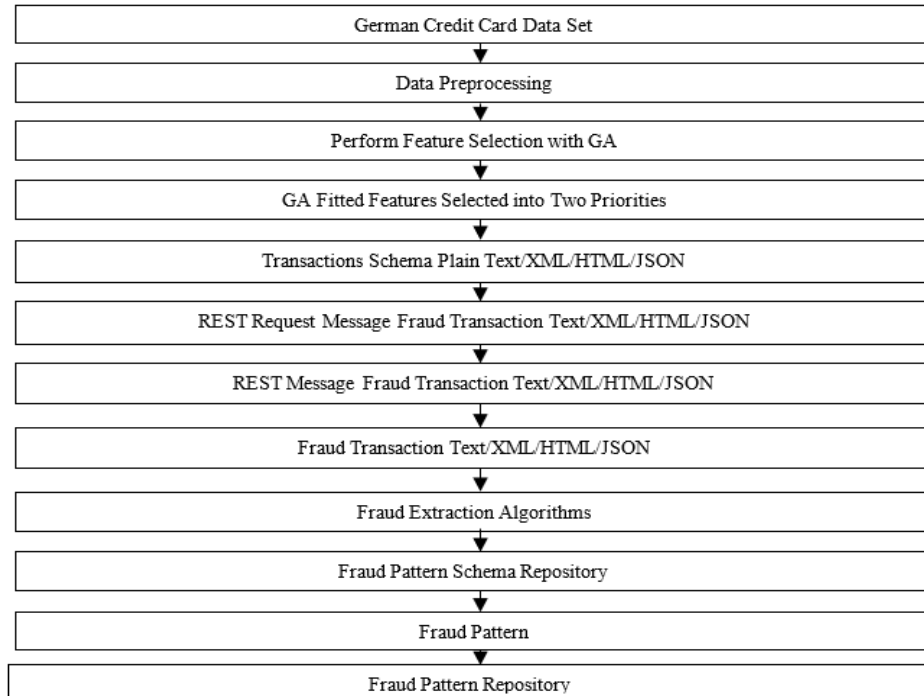


Figure 1. The block diagram of presented prevention of CCF transaction using GA feature selection

GA: one of the most popular approaches for analysing evolutionary computation is the GA methodology. It duplicates the process of natural selection. It is widely utilised in a range of industries, including business, engineering, and others. Finding the best answer to an issue is the intended course of

action. Three basic operators make up GA: crossing, mutation, and selection. Based on fitness function, selection takes the fitness values and separates them from the available population set. In crossover, the latter half of the first record is mixed with the first half. Every 0 is replaced with a 1 through random mutation. The following are the steps involved in GA: generate a population of random chromosomal 'n' individuals, each with a unique response to the challenge. Determine each 'x' chromosome's fitness. Create a new population up to the point of completeness.

Selection: dependent on the genes of both parents, choose a higher fitness value. To produce new offspring so the parents can interbreed. It can have multiple points or only one. Mutation: In the process of mutation, a few bits randomly flip to create new offspring. The acceptance phase is imposed on a newly arrived population. To do the replacement step computation, use a new population. The final prerequisite is satisfied, stop the testing phase and reinstate the ideal configuration for the present population. Continue on to the looping phases step 2. In order to characterize the architectural style that is used to communicate the web services known as RESTful web services, Roy Fielding developed the word "REST" (representational state transfer). A loosely connected web of lightweight, fast, and scalable services is built using the architectural design pattern known as REST.

Because enveloping is not necessary, there is very little overhead in the header data for the REST request message, which reduces the message's size and speeds up transport as compared to simple object access protocol (SOAP) messages. The following are the architectural constraints when creating REST web services: each resource in the system should have the same interface, which implies it should have just one URI. Client-server separation calls for independence between the client and the server. Only requests and answers are exchanged between individuals. Statelessness: there is no storage of server-side sessions. Resources that can be cached: the server's answers should include information regarding the data's cache ability. If resources are cacheable, the version number should be disclosed along with each other. Between the client and the server, multiple servers might exist, but neither the request nor the reaction should be impact.

The executable code, which is executed by the sender, is contained in the code on demand (optional). The fraudulent transaction flow in a REST-based online service is represented in the diagram using JavaScript object notation (JSON) format. The fraudulent transaction pattern is requested by the service consumer from the service provider through metadata exchange. REST clients and servers can communicate with one another across a wide range of platforms because of their loose connectivity. Due to the close coupling of SOAP clients, any modifications to either the server or the client could allow the integration between them to fail. Here, the fraud extraction methods are used.

Machine learning, statistical analysis, and behaviour tracking are used to identify fraud schemes and criminals' methods. The system can prevent fraudulent behaviour before any harm is done when fraud indicators are found. Finding patterns with the help of a machine learning system is known as pattern recognition. It's the grouping of information according to previous experience or statistical information obtained from patterns and/or their presentation.

Firstly, the German data set is collected and preprocessed to clean the data. After that feature selection with GA is performed to eliminate the duplication and improve the accuracy. The GA algorithm divided the data into two priorities to identify whether a fraud is happened or not. The data may be in any for plain text /HTML/JSON/XML. The architectural style known as RESTful web services is used to communicate with web services, and it is referred to by the word REST. The REST sends the message to either a fraud transaction is happened or not on web-based application. If any fraud transaction will happen then fraud extraction algorithm is used to extract the fraud features. Fraud pattern recognition is used to identify what patterns are used by fraudsters. Based on the identified pattern, appropriate action is taken to prevent the fraudster before any harm.

3. RESULT ANALYSIS

The prevention of CCF transaction using GA feature selection is demonstrated in this part with an example of the outcome analysis. Accuracy, recall, and specificity are used to assess the efficiency of the model that is being presented. True positive (TP), true negative (TN), false negative (FN), and false positive (FP) are defined as follows:

- TP: TP is the total number of positive predictive occurrences that are all correctly classified as positive predictions.
- TN: the term "TN" refers to the total number of correctly classified, actually negative predicted instances.
- FP: the total number of instances of positive predictions that are FP characterised as creating error and are not actually positive.

– FP: the number of negative predictive instances, or FN, that are reasonable yet completely incorrectly classified is given.

Accuracy: it is given in (1) and is defined as the ratio of accurately detected occurrences to all instances.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \times 100 \tag{1}$$

Recall: showed us methods to locate every pertinent instance in a dataset. In other words, (2) describes categorization models, which identify every relevant instances.

$$Recall = \frac{TP}{TP+FN} \times 100 \tag{2}$$

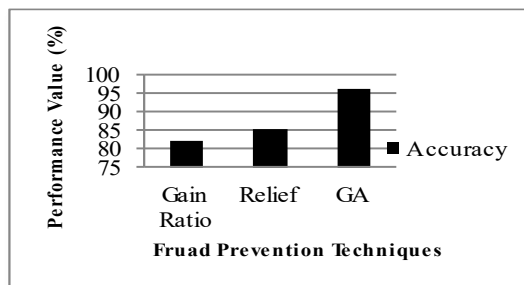
Specificity: it is described as the true negative instances to the actual negative instances (i.e. FP+TN) and is expressed in (3).

$$Specificity = \frac{TN}{TN+FP} \times 100 \tag{3}$$

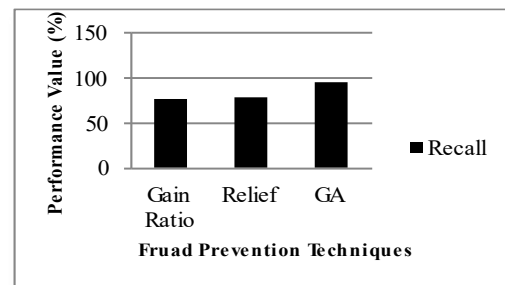
The given prevention of CCF transaction utilising GA feature selection for web-based applications is described in the Table 1 performance analysis. The above table demonstrates that the GA, which is used to identify CCFs for web-based with the highest accuracy, recall, and specificity. The Figure 2 shows the performance comparative graph in terms of Accuracy and Recall. The Figure 2(a) shows accuracy and Figure 2(b) shows recall comparison. In Figure 2(a) the results shows that GA feature selection has higher accuracy. From the Figure 2(b), it is observed that, GA feature selection has higher recall. The Figure 3 shows Specificity performance comparison. Presented GA approach has high specificity than other algorithms as shown in Figure 3. Thus, the proposed method for using the selection of GA features for web-based applications to stop CCF transactions has successfully discovered the frauds and stopped them before any harm had occurred.

Table 1. Performance analysis

Performance metrics	Gain ratio	Relief	GA
Accuracy (%)	82.34	85.56	96.12
Recall (%)	76.65	78.68	95.64
Specificity (%)	82.68	80.97	89.95



(a)



(b)

Figure 2. Comparative graph for (a) accuracy and (b) recall

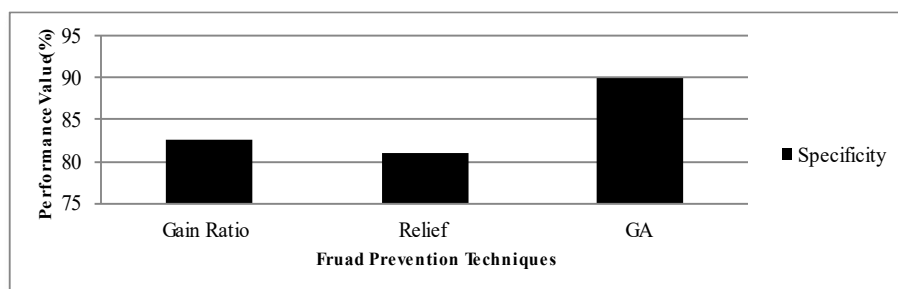


Figure 3. Specificity performance comparison between methods

4. CONCLUSION

Experts have been interested in identifying CCF for a long time. This is mostly caused by the ongoing alteration of fraud pattern. Credit cards are becoming a common method of payment due to recent technological advancements. Fraud has grown to unmanageable levels as a result of operational security issues, causing annual losses in the millions of dollars. As a result, a fraud detection and prevention strategy are required to reduce credit card payment fraud. To provide better prevention techniques for CCF, prevention of CCF transaction using GA feature selection for web-based application is presented. In this work, German credit card dataset is used. Collected data is preprocessed to remove the noise and clean the data. This method presented CCF identification with the use of GA feature selection. Based on the data, it was clear that GA outperformed other feature selection techniques in terms of first priority feature selection accuracy. This method's performance is determined by a number of factors, including specificity, accuracy, and recall. The results demonstrate that the proposed use of GA feature selection for web-based applications to prevent CCF transactions has produced better results than previous methods in terms of accuracy, recall, and specificity. As a future work, a hybrid feature selection model with deep learning for effective prevention of CCF will be implemented.




REFERENCES

- [1] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 1, pp. 362–373, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp362-373.
- [2] Y. Xie, G. Liu, C. Yan, C. Jiang, and M. Zhou, "Time-aware attention-based gated network for credit card fraud detection by extracting transactional behaviors," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 3, pp. 1004–1016, Jun. 2023, doi: 10.1109/TCSS.2022.3158318.
- [3] E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost," *IEEE Access*, vol. 9, pp. 165286–165294, 2021, doi: 10.1109/ACCESS.2021.3134330.
- [4] E. Strelcenia and S. Prakoonwit, "Improving classification performance in credit card fraud detection by using new data augmentation," *AI*, vol. 4, no. 1, pp. 172–198, Jan. 2023, doi: 10.3390/ai4010008.
- [5] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit card fraud detection using a new hybrid machine learning architecture," *Mathematics*, vol. 10, no. 9, p. 1480, Apr. 2022, doi: 10.3390/math10091480.
- [6] I. Sadgali, N. Sael, and F. Benabbou, "Bidirectional gated recurrent unit for improving classification in credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 21, no. 3, pp. 1704–1712, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1704-1712.
- [7] R. Asha and S. K. Kumar, "Credit card fraud detection using artificial neural network," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35–41, Jun. 2021, doi: 10.1016/j.gltp.2021.01.006.
- [8] A. Razaque *et al.*, "Credit card-not-present fraud detection and prevention using big data analytics algorithms," *Applied Sciences*, vol. 13, no. 1, p. 57, Dec. 2022, doi: 10.3390/app13010057.
- [9] A. A. Basori and N. H. M. Ariffin, "The adoption factors of two-factors authentication in blockchain technology for banking and financial institutions," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 3, pp. 1758–1764, Jun. 2022, doi: 10.11591/ijeecs.v26.i3.pp1758-1764.
- [10] D. Lunghi, G. M. Paldino, O. Caelen, and G. Bontempi, "An adversary model of fraudsters' behavior to improve oversampling in credit card fraud detection," *IEEE Access*, vol. 11, pp. 136666–136679, 2023, doi: 10.1109/ACCESS.2023.3337635.
- [11] A. Priyadarshini, S. Mishra, D. P. Mishra, S. R. Salkuti, and R. Mohanty, "Fraudulent credit card transaction detection using soft computing techniques," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 23, no. 3, pp. 1634–1642, Sep. 2021, doi: 10.11591/ijeecs.v23.i3.pp1634-1642.
- [12] I. D. Mienye and Y. Sun, "A machine learning method with hybrid feature selection for improved credit card fraud detection," *Applied Sciences*, vol. 13, no. 12, p. 7254, Jun. 2023, doi: 10.3390/app13127254.
- [13] Arati Shahapurkar, Rudragoud Patil, "Concept drift and machine learning model for detecting fraudulent transactions in streaming environment," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 5, pp. 5560–5568, October 2023, doi: 10.11591/ijece.v13i5.pp5560-5568
- [14] N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning," *Electronics*, vol. 11, no. 4, p. 662, Feb. 2022, doi: 10.3390/electronics11040662.
- [15] M. Zanin, M. Romance, S. Moral, and R. Criado, "Credit card fraud detection through parenclitic network analysis," *Complexity*, vol. 2018, pp. 1–9, 2018, doi: 10.1155/2018/5764370.
- [16] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit card fraud detection using AdaBoost and majority voting," *IEEE Access*, vol. 6, pp. 14277–14284, 2018, doi: 10.1109/ACCESS.2018.2806420.
- [17] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," *IEEE Access*, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.
- [18] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine," *IEEE Access*, vol. 8, pp. 25579–25587, 2020, doi: 10.1109/ACCESS.2020.2971354.
- [19] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.
- [20] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "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, Aug. 2018, doi: 10.1109/TNNLS.2017.2736643.
- [21] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.
- [22] R. Sailusha, V. Gnaneshwar, R. Ramesh, and G. R. Rao, "Credit card fraud detection using machine learning," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, May 2020, pp. 1264–1270, doi: 10.1109/ICICCS48265.2020.9121114.




- [23] S. Patil, V. Nemade, and P. K. Soni, "Predictive modelling for credit card fraud detection using data analytics," *Procedia Computer Science*, vol. 132, pp. 385–395, 2018, doi: 10.1016/j.procs.2018.05.199.
- [24] J. R. D. Kho and L. A. Ve, "Credit card fraud detection based on transaction behavior," in *TENCON 2017 - 2017 IEEE Region 10 Conference*, Nov. 2017, pp. 1880–884, doi: 10.1109/TENCON.2017.8228165.
- [25] S. K. Babu, S. Vasavi, and K. Nagarjuna, "Framework for predictive analytics as a service using ensemble model," in *2017 IEEE 7th International Advance Computing Conference (IACC)*, Jan. 2017, pp. 121–128, doi: 10.1109/IACC.2017.0038.
- [26] Varun Kumar K S, "Credit card fraud detection using machine learning algorithms," *International Journal of Engineering Research and*, vol. V9, no. 07, pp. 1526–1530, Aug. 2020, doi: 10.17577/IJERTV9IS070649.
- [27] Y. Ding, W. Kang, J. Feng, B. Peng, and A. Yang, "Credit card fraud detection based on improved variational autoencoder generative adversarial network," *IEEE Access*, vol. 11, pp. 83680–83691, 2023, doi: 10.1109/ACCESS.2023.3302339.
- [28] H. Wang, W. Wang, Y. Liu, and B. Alidaee, "Integrating machine learning algorithms with quantum annealing solvers for online fraud detection," *IEEE Access*, vol. 10, pp. 75908–75917, 2022, doi: 10.1109/ACCESS.2022.3190897.

BIOGRAPHIES OF AUTHORS






Kavuri Sreekanth    is presently working as Assistant Professor in the Department of Computer Science and Engineering at Koneru Lakshmaiah Deemed to be University. Previously he worked as an employee in AP state government university and taught many subjects in Computer Science and Engineering Department and Information Technology department. He completed his Post Graduation from JNTU Hyderabad. Pursuing Research in the area of web mining. He can be contacted at email: kavurikanth@gmail.com.






Dr. Ratnababu Mamidi    received B. Tech from JNTU, Hyderabad. The M.E. Degree from M.S. University of Baroda, Vadodara and Ph.D. from IIT-Bombay, Mumbai. He held different administrative posts with several engineering colleges. He is presently working as Professor with St.ann's College of Engineering and Technology, Andhra Pradesh. He can be contacted at email: mamidi.ratnababu@gmail.com.






Dr. Thumu Srinivas Reddy    is currently working as an associate professor in Malla Reddy Engineering College, Main Campus, Dhulapally. His highest qualification is Ph.D. He has 17 years of experience. He has published 19 publications in reputed international journal publications. He participated in different international conferences during the years, 2016, 2017, and 2018. He can be contacted at email: srinivasreddy.thumu@gmail.com.



Dr. Kuruva Maddileti    B.Sc. degree in Mathematical Science from the Sri Krishna Devaraya University, the M.Sc. degree in Mathematics from the Sri Venkateswara University and the Ph.D. degree in mathematics from the EILMU University. He used to hold several administrative posts with mathematics in Shanthinikethan College of Education, Rayala Seema University from 2015 to 2023. He completed B.Ed. and M.Ed. from Sri Krishna Devaraya University, Ananthapur. He is currently a associate professor with the Department of Humanities and Basic Sciences Mathematics and applied mathematics in Dr.K.V. Subba Reddy Institute of Technology. He has authored six journals. He has research interest in mathematics. He can be contacted at email: kmaddiletibed@gmail.com.



Darivemula Deepthi    received the B. Tech Degree in Computer Science and Engineering from Vathsalya Institute Of Science and Technology in 2005, M. Tech Degree from Sir C.R.Reddy College of Engineering in 2012. Currently, pursuing Ph.D. degree from Andhra University (AU) Under the guidance of Dr. Padma Bhogaraju, associate professor from GVP Degree and PG College, Vizag, A.P. Her areas of interests are in cryptography and network security. She can be contacted at email: 10.deepthi@gmail.com.