ISSN 2347–3657

Volume 13, Issue 2s, 2025

AI BASED CREDIT SCORING SYSTEM WITH DYNAMIC RISK ASSESSMENT

[1]Mohammed Azmath ulla khan, [2]Mohammad Musaddiq, [3]Mohammed Faizan, [4]Heena Yasmeen.
[1,2,3]B.E Students, Department Of Information Technology, ISL Engineering College, Hyderabad, India.
[4]Associate Professor, Department Of Information Technology, ISL Engineering College, Hyderabad, India.
ullakhanazmath@gmail.com

ABSTRACT

Credit cards are now potentially the most popular mode of payment for both offline and online purchases thanks to new developments in electronic commerce systems and communication technology; as a result, there is much more fraud involved with such transactions. Every year, fraudulent credit card transactions cause businesses and individuals to lose a lot of money, and con artists are constantly looking for new tools and techniques to commit fraud. Researchers face a difficult task when trying to identify credit card theft since criminals are quick-thinking and inventive. The dataset provided for credit card fraud detection is severely unbalanced, making it difficult for the system to detect fraud. The use of credit cards is quite important in today's economy. It is an essential component of every family, company, and global enterprise. While using credit cards responsibly and safely can have many benefits, engaging in fraudulent behaviour can have a negative impact on your credit and finances. There have been several solutions proposed to address the escalating credit card theft. The increased use of electronic payments is now significantly impacted by the detection of fraudulent transactions. As a result, methods that are efficient and effective for identifying fraud in credit card transactions are required. Gradient Boosting Classifier, a machine learning methodology, is suggested in this research as a smart method for identifying fraud in credit card transactions. The experimental results show that the suggested approach worked better than other machine learning algorithms and reached the maximum accuracy performance, with training accuracy of 100% and test accuracy of 91%

1-INTRODUCTION

Credit card fraud (CCF) is a type of identity theft in which someone other than the owner makes an unlawful transaction using a credit card or account details. A credit card that has been stolen, lost, or counterfeited might result in fraud. Card-not-present fraud, or the use of your credit card number in e-commerce transactions has also become increasingly common as a result of the increase in online shopping. Increased fraud, such as CCF, has resulted from the expansion of e-banking and several online payment environments, resulting in annual losses of billions of dollars. In this era of digital payments, CCF detection has become one of the most important goals. As a business owner, it cannot be disputed that the future is heading towards a cashless culture. As a result, typical payment methods will no longer be used in the future, and therefore they will not be helpful for expanding a business. Customers will not always visit the business with cash in their pockets. They are now placing a premium on debit and credit card payments. As a result, companies will need to update their environment to ensure that they can take all types of payments. In the next years, this situation is expected to become much more severe.

ML models have been used in many studies to solve numerous challenges. Deep learning (DL) algorithms applied applications in computer network, intrusion detection, banking, insurance, mobile cellular networks, health care fraud detection, medical and malware detection, detection for video surveillance, location tracking, Android malware detection, home automation, and heart disease prediction. We explore the practical application of ML, particularly DL algorithms, to identify credit card thefts in the banking industry in this paper.

1.2 SCOPE OF THE PROJECT

The scope of this study is to investigate the application of Gradient Boosting Classifier, a machine learning algorithm, to detect credit card fraud in the banking industry. The study will focus on the practical implementation of the algorithm and its effectiveness in identifying fraudulent

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

transactions. The results of this research can be used to develop a system that can accurately detect credit card fraud and help prevent financial losses for individuals and businesses.

1.3 OBJECTIVE

The objective of this study is to apply machine learning algorithms, particularly Gradient Boosting Classifier, for credit card fraud detection in the banking industry. The study aims to overcome the challenges of identifying credit card theft, such as unbalanced datasets and quick-thinking criminals. The focus is on developing an efficient and effective method for detecting fraudulent transactions to minimize the losses incurred by businesses and individuals due to credit card fraud. The study seeks to compare the performance of Gradient Boosting Classifier with other machine learning algorithms commonly used for credit card fraud detection. Furthermore, the study aims to highlight the importance of fraud detection in the context of the increasing use of electronic payments and the need for businesses to update their environments to accommodate various payment methods. Finally, the study intends to contribute to the development of advanced fraud detection techniques in the banking industry

1.4 EXISTING SYSTEM:

- Frauds in credit card transactions are common today as most of us are using the credit card payment methods more frequently. This is due to the advancement of Technology and increase in online transaction resulting in frauds causing huge financial loss.
- Therefore, there is need for effective methods to reduce the loss. In addition, fraudsters find ways to steal the credit card information of the user by sending fake SMS and calls, also through masquerading attack, phishing attack and so on. This paper aims in using the multiple algorithms of Machine learning such as convolutional neural network (CNN), k-nearest neighbor (Knn) and artificial neural network (ANN) in predicting the occurrence of the fraud.

1.4.1 EXISTINGSYSTEM DISADVANTAGES:

- It needed high processing time for big neural networks.
- It training requires lots of data.

It requires lots of computational power.

2-LITERATURE SURVEY

Title: An efficient real time model for credit card fraud detection based on deep learning.
Author: Y. Abakarim, M. Lahby, and A. Attioui
Year: 2021.
Description: In the last decades Machine Learning achieved notable results in various areas of data processing and classification, which made the creation of real-time interactive and intelligent systems possible. The accuracy and precision of those systems depends not only on the correctness of the data, logically and chronologically, but also on the time the feed-backs are produced. This paper focuses on one of these systems which is a fraud detection system. In order to have a more accurate and precise fraud detection system, banks and financial institutions are investing more and more today in perfecting the algorithms and data analysis technologies used to identify and combat fraud. Therefore, many solutions and algorithms using machine learning have been proposed in literature to deal with this issue. However, comparison studies exploring Deep learning paradigms are scarce, and to our knowledge, the proposed works don't consider the importance of a Real-time approach for this type of problems. Thus, to cope with this problem we propose a live credit card fraud detection system based on a deep neural network technology. Our proposed model is based on an auto-encoder and it permits to classify, in real-time, credit card transactions as legitimate or fraudulent. To test the effectiveness of our model, four different binary classification models are used as a comparison. The Benchmark shows promising results for our proposed model than existing solutions in terms of accuracy, recall and precision

Title: Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence
Author: V. Arora, R. S. Leekha, K. Lee, and A. Kataria
Year: 2020.
Description: An effective machine learning implementation means that artificial intelligence has tremendous potential to help and automate financial

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

threat assessment for commercial firms and credit agencies. The scope of this study is to build a predictive framework to help the credit bureau by modelling/assessing the credit card delinquency risk. Machine learning enables risk assessment by predicting deception in large imbalanced data by classifying the transaction as normal or fraudster. In case of fraud transaction, an alert can be sent to the related financial organization that can suspend the release of payment for particular transaction. Of all the machine learning models such as RUSBoost, decision tree, logistic regression, multilayer perceptron, K-nearest neighbor, random forest, and support vector machine, the overall predictive performance of customized RUSBoost is the most impressive. The evaluation metrics used in the experimentation are sensitivity, specificity, precision, F scores, and area under receiver operating characteristic and precision recall curves. Datasets used for training and testing of the models have been taken from kaggle.com.

Title: Performance analysis of feature selection methods in software defect prediction: A search method approach
Author: A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim
Year: 2019.
Description: Software Defect Prediction (SDP) models are built using software metrics derived from software systems. The quality of SDP models depends largely on the quality of software metrics (dataset) used to build the SDP models. High dimensionality is one of the data quality problems that affect the performance of SDP models. Feature selection (FS) is a proven method for addressing the dimensionality problem. However, the choice of FS method for SDP is still a problem, as most of the empirical studies on FS methods for SDP produce contradictory and inconsistent quality outcomes. Those FS methods behave differently due to different underlining computational characteristics. This could be due to the choices of search methods used in FS because the impact of FS depends on the choice of search method. It is hence imperative to comparatively analyze the FS methods performance based on different search methods in SDP. In this paper, four filter feature ranking (FFR) and fourteen filter feature subset selection (FSS) methods were evaluated using four different classifiers over five software defect datasets obtained from the National Aeronautics and Space Administration (NASA) repository. The experimental analysis showed that the application of FS improves the predictive performance of classifiers and the performance of FS methods can vary across datasets and classifiers. In the FFR methods, Information Gain demonstrated the greatest improvements in the performance of the prediction models. In FSS methods, Consistency Feature Subset Selection based on Best First Search had the best influence on the prediction models. However, prediction models based on FFR proved to be more stable than those based on FSS methods.

Title: Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia
Author: B. Bandaranayake
Year: 2014
Description: This case describes the implementation of a fraud and corruption control policy initiative within the Victorian Department of Education and Early Childhood Development (the Department) in Australia. The policy initiative was administered and carried out by a small team of fraud control officials, including the author of this article, in the Department. The policy context represents a large, devolved and fragmented governance and accountability system. This case highlights the complexity of the policy initiative, the contextual constraints that challenged the implementation, and the pragmatic approach taken by the Department. While there are no easy solutions for fraud and corruption control or proven models to follow, this case presents helpful lessons for the professionals working in large and devolved education systems.

Title: Credit card fraud detection model based on LSTM recurrent neural networks
Author: I. Benchaji, S. Douzi, and B. E. Ouahidi
Year: 2021.
Description: With the increasing use of credit cards in electronic payments, financial institutions and service providers are vulnerable to fraud, costing huge losses every year. The design and the implementation of efficient fraud detection system is essential to reduce such **losses.** However, machine learning techniques used to detect automatically card fraud do not consider fraud sequences or behavior changes which may lead to false alarms. In this paper, we develop a credit card fraud detection system that employs Long **Short-**Term Memory (LSTM) networks as a sequence

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

learner to include transaction sequences. The proposed approach aims to capture the historic purchase behavior of credit card holders with the goal of improving fraud detection accuracy on new incoming transactions. Experiments show that our proposed model gives strong results and its accuracy is quite high..1.6 PROPOSED SYSTEM

- In recent years, deep learning approaches have received significant attention due to substantial and promising out-comes in various applications, such as computer vision, natural language processing, and voice. However, only a few studies have examined the application of deep neural net-works in identifying CCF. [3]. It uses a number of deep learning algorithms for detecting CCF.
- However, in this study, we choose the Gradient Boosting Classifier model and its layers to determine if the original fraud is the normal transaction of qualified datasets. Some transactions are common in datasets that have been labelled fraudulent and demonstrate questionable transaction behaviour. As a result, we focus on Gradient Boosting Classifier learning in this research paper.

1.6.1 PROPOSED SYSTEM ADVANTAGES:

- It has an in-built capability to handle missing values.
- It is generally used when we want to decrease the Bias error.

PROJECT DESCRIPTION

2.1 GENERAL:

This project aims to develop a machine learning model using Gradient Boosting Classifier to detect credit card fraud in the banking industry. The model will be trained on a large dataset of credit card transactions and will be tested for accuracy and efficiency in identifying fraudulent transactions. The ultimate goal is to provide a tool that can be used by financial institutions to prevent credit card fraud and minimize financial losses.

3-METHODOLOGY

MODULES NAME:

- **Data Collection**
- **Dataset**
- **Data Preparation**
- **Model Selection**
- **Analyze and Prediction**
- **Accuracy on test set**
- **Saving the Trained Mod**

MODULES DESCSRIPTION:

1) Data Collection:

This is the first real step towards the real development of a machine learning model, collecting data. This is a critical step that will cascade in how good the model will be, the more and better data that we get, the better our model will perform.

There are several techniques to collect the data, manual interventions and etc. Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms

2) Dataset:

The dataset consists of 1000 individual data. There are 21 columns in the dataset.

3) Data Preparation:

Wrangle data and prepare it for training. Clean that which may require it (remove duplicates, correct errors, deal with missing values, normalization, data type conversions, etc.)

Randomize data, which erases the effects of the particular order in which we collected and/or otherwise prepared our data

Visualize data to help detect relevant relationships between variables or class imbalances (bias alert!), or perform other exploratory analysis

Split into training and evaluation sets

4) Model Selection:

We used Gradient Boosting Classifier machine learning algorithm, We got a accuracy of 91 % on test set so we implemented this algorithm.

5) Analyze and Prediction:

In the actual dataset, we chose only 14 features:

- **credit_usage :** Users credit usage
- **credit_history :** Users credit history
- **purpose :** Users purpose
- **current_balance :** Users current balance
- **Average_Credit_Balance :** Users average credit balance

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

ISSN 2347–3657

Volume 13, Issue 2s, 2025

- **personal_status :** Users personal status
- **other_parties :** Other parties
- **property_magnitude:** Users Property
- **cc_age :** Users age
- **other_payment_plans :** payment plans
- **housing :** housing types
- **job :** job types
- **num_dependents :** Numbers of dependents
- **foreign_worker :** Foreign worker yes or no
- **Class:** Good or Bad

6) Accuracy on test set:
We got an accuracy of 91.7% on test set.

7) Saving the Trained Model:
Once you're confident enough to take your trained and tested model into the production-ready environment, the first step is to save it into a .h5 or .pkl file using a library like pickle.
Make sure you have pickle installed in your environment.
Next, let's import the module and dump the model into .pkl file.

2.3 TECHNIQUE USED OR ALGORITHM USED

2.3.1 EXISTING TECHNIQUE: -

- ➢ **Artificial Neural Network (ANN)**

- ➢ We have used the neural network, even though tough to train the model which would fit fine to model for detecting a fraud in credit card Transactions. In our model, by using an artificial neural network (ANN) which gives accuracy approximately equal to 100% is best suited for credit card fraud detection.

- ➢ ANN is biologically inspired by human brain. The neurons are interconnected in the human brain like the same nodes are interconnected in artificial neural network. ANN with input, output and hidden layers. Inputs are x1, x2…Xn and output is y. w1…wn are the weights associated with inputs x1…xn respectively. There are 15 hidden layers used in this neural network. The activation function used in our credit card fraud detection model is RELU

2.3.2 PROPOSED TECHNIQUE USED OR ALGORITHM USED:

- ➢ **Gradient Boosting Classifier.**
- ➢ Gradient boosting algorithm can be used for predicting not only continuous target variable (as a Regressor) but also categorical target variable (as a Classifier). When it is used as a regressor, the cost function is Mean Square Error (MSE) and when it is used as a classifier then the cost function is Log loss.
- ➢ In order to make initial predictions on the data, the algorithm will get the log of the odds of the target feature. This is usually the number of True values(values equal to 1) divided by the number of False values(values equal to 0)..

4-REQUIREMENTS ENGINEERING

GENERAL

We can see from the results that on each database, the error rates are very low due to the discriminatory power of features and the regression capabilities of classifiers. Comparing the highest accuracies (corresponding to the lowest error rates) to those of previous works, our results are very competitive.

3.2 HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It should what the system do and not how it should be implemented.

• PROCESSOR	:	DUAL CORE 2 DUOS.
• RAM	:	4GB DD RAM
• HARD DISK	:	250 GB

3.3 SOFTWARE REQUIREMENTS

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity.

- Operating System : Windows 7/8/10
- Platform : Spyder3
- Programming Language : Python
- Front End : HTML, CSS

3.4 FUNCTIONAL REQUIREMENTS

A functional requirement defines a function of a software-system or its component. A function is described as a set of inputs, the behavior, Firstly, the system is the first that achieves the standard notion of semantic security for data confidentiality in attribute-based deduplication systems by resorting to the hybrid cloud architecture.

3.5 NON-FUNCTIONAL REQUIREMENTS

The major non-functional Requirements of the system are as follows

Usability

The system is designed with completely automated process hence there is no or less user intervention.

Reliability

The system is more reliable because of the qualities that are inherited from the chosen platform python. The code built by using python is more reliable.

Performance

This system is developing in the high level languages and using the advanced back-end technologies it will give response to the end user on client system with in very less time.

Supportability

The system is designed to be the cross platform supportable. The system is supported on a wide range of hardware and any software platform, which is built into the system.

Implementation

The system is implemented in web environment using Jupyter notebook software. The server is used as the intellignce server and windows 10 professional is used as the platform. Interface the user interface is based on FLASK provides server system.

DESIGN ENGINEERING

GENERAL:

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering.

IMPLEMENTATION

CLASS DIAGRAM :

7-CONCLUSION

The prevention of credit card fraud is essential for increased credit card use. The financial losses suffered by financial institutions are significant and ongoing, and the detection of credit card fraud is becoming more challenging, thus it is crucial to create more efficient methods for doing so. Gradient Boosting Classifier is used in this paper to suggest an intelligent method for identifying fraud in credit card transactions. We performed a number of experiments utilising actual data. Performance analysis metrics were used to assess the performance of the suggested approach. According to the experimental findings, the suggested method outperformed other machine learning algorithms and attained the maximum accuracy performance. The outcomes demonstrate that the suggested method outperforms alternative classifiers. The outcomes further emphasise the significance and benefit of implementing an effective parameter optimization strategy for boosting the suggested approach's predictive capabilities.

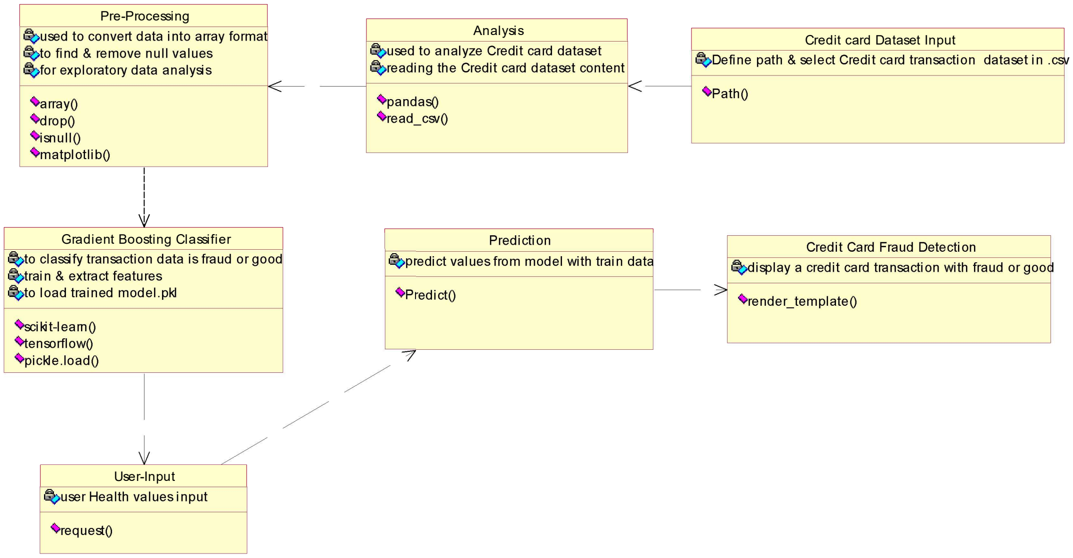
10.2 REFERENCES

[1] Y. Abakarim, M. Lahby, and A. Attioui, ``An effficient real time model for credit card fraud detection based on deep learning," in Proc. 12th Int. Conf. Intell. Systems: Theories Appl., Oct. 2018, pp. 17, doi: 10.1145/3289402.3289530.

[2] H. Abdi and L. J. Williams, ``Principal component analysis,'' Wiley Interdiscipl. Rev., Comput. Statist., vol. 2, no. 4, pp. 433459, Jul. 2010, doi: 10.1002/wics.101.

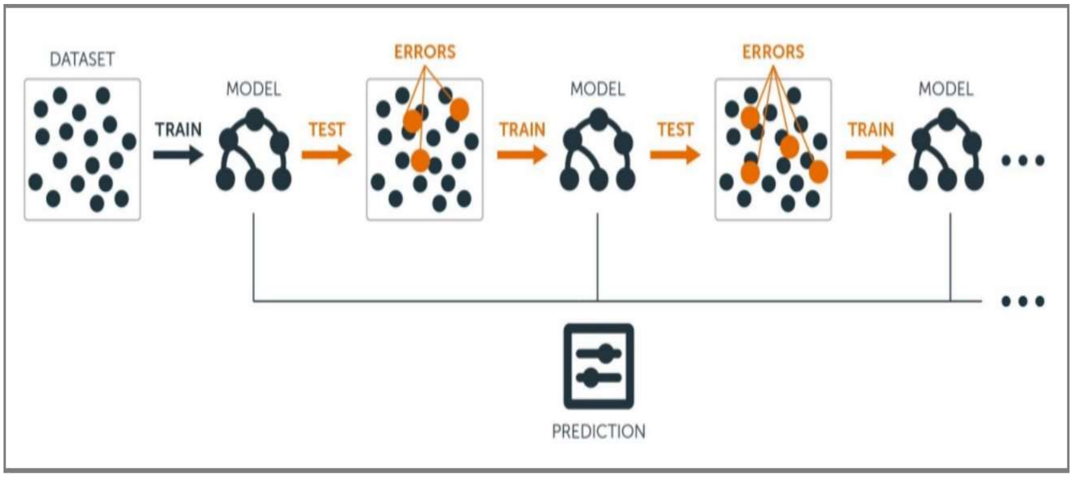
[3] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, ``Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence,'' Mobile Inf. Syst., vol. 2020, pp. 113, Oct. 2020, doi: 10.1155/2020/8885269.

[4] A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, ``Performance analysis of feature selection selection methods in software defect prediction: A search method approach,'' Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.


Pre-Processing
used to convert data into array format
to find & remove null values
for exploratory data analysis
array()
drop()
isnull()
matplotlib()
Analysis
used to analyze Credit card dataset
reading the Credit card dataset content
pandas()
read_csv()
Credit card Dataset Input
Define path & select Credit card transaction dataset in .csv
Path()
Gradient Boosting Classifier
to classify transaction data is fraud or good
train & extract features
to load trained model.pkl
scikit-learn()
tensorflow()
pickle.load()
Prediction
predict values from model with train data
Predict()
Credit Card Fraud Detection
display a credit card transaction with fraud or good
render_template()
User-Input
user Health values input
request()

In this class diagram represents how the classes with attributes and methods are linked together to perform the verification with security. From the above diagram shown the various classes involved in our project.

SYSTEM ARCHITECTURE:



DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

[5] B. Bandaranayake, ``Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia,'' J. Cases Educ. Leadership, vol. 17, no. 4, pp. 3453, Dec. 2014, doi: 10.1177/1555458914549669.

[6] J. Bªaszczy«ski, A. T. de Almeida Filho, A. Matuszyk, M. Szelg
, and R. Sªowi«ski, ``Auto loan fraud detection using dominance-based rough set approach versus machine learning methods,'' Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[7] B. Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão, and P. Bizarro, ``Interleaved sequence RNNs for fraud detection,'' in Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2020, pp. 31013109, doi: 10.1145/3394486.3403361.

[8] F. Cartella, O. Anunciacao, Y. Funabiki, D. Yamaguchi, T. Akishita, and O. Elshocht, ``Adversarial attacks for tabular data: Application to fraud detection and imbalanced data,'' 2021, arXiv:2101.08030.

[9] S. S. Lad, I. Dept. of CSE Rajarambapu Institute of Technology Rajaramnagar Sangli Maharashtra, and A. C. Adamuthe, ``Malware classification with improved convolutional neural network model,'' Int. J. Comput. Netw. Inf. Secur., vol. 12, no. 6, pp. 3043, Dec. 2021, doi: 10.5815/ijcnis.2020.06.03.

[10] V. N. Dornadula and S. Geetha, ``Credit card fraud detection using machine learning algorithms,'' Proc. Comput. Sci., vol. 165, pp. 631641, Jan. 2019, doi: 10.1016/j.procs.2020.01.057.

[11] I. Benchaji, S. Douzi, and B. E. Ouahidi, ``Credit card fraud detection model based on LSTM recurrent neural networks,'' J. Adv. Inf. Technol., vol. 12, no. 2, pp. 113118, 2021, doi: 10.12720/jait.12.2.113-118.

[12] Y. Fang, Y. Zhang, and C. Huang, ``Credit card fraud detection based on machine learning,'' Comput., Mater. Continua, vol. 61, no. 1, pp. 185195, 2019, doi: 10.32604/cmc.2019.06144.

[13] J. Forough and S. Momtazi, ``Ensemble of deep sequential models for credit card fraud detection,'' Appl. Soft Comput., vol. 99, Feb. 2021, Art. no. 106883, doi: 10.1016/j.asoc.2020.106883.

[14] K. He, X. Zhang, S. Ren, and J. Sun, ``Deep residual learning for image recognition,'' 2015, arXiv:1512.03385.

[15] X. Hu, H. Chen, and R. Zhang, ``Short paper: Credit card fraud detection using LightGBM with asymmetric error control,'' in Proc. 2nd Int. Conf. Artif. Intell. for Industries (AII), Sep. 2019, pp. 9194, doi:10.1109/AI4I46381.2019.00030.

[16] J. Kim, H.-J. Kim, and H. Kim, ``Fraud detection for job placement using hierarchical clusters-based deep neural networks,'' Int. J. Speech Technol., vol. 49, no. 8, pp. 28422861, Aug. 2019, doi: 10.1007/s10489-019-01419-2.

[17] M.-J. Kim and T.-S. Kim, ``A neural classier with fraud density map for effective credit card fraud detection,'' in Intelligent Data Engineering and Automated Learning, vol. 2412, H. Yin, N. Allinson, R. Freeman, J. Keane, and S. Hubbard, Eds. Berlin, Germany: Springer, 2002, pp. 378383, doi: 10.1007/3-540-45675-9_56.

[18] N. Kousika, G. Vishali, S. Sunandhana, and M. A. Vijay, ``Machine learning based fraud analysis and detection system,'' J. Phys., Conf., vol. 1916, no. 1, May 2021, Art. no. 012115, doi: 10.1088/1742-6596/1916/1/012115.

[19] R. F. Lima and A. Pereira, ``Feature selection approaches to fraud detection in e-payment systems,'' in E-Commerce and Web Technologies, vol. 278, D. Bridge and H. Stuckenschmidt, Eds. Springer, 2017, pp. 111126, doi: 10.1007/978-3-319-53676-7_9.

[20] Y. Lucas and J. Jurgovsky, ``Credit card fraud detection using machine learning: A survey,'' 2020, arXiv:2010.06479.

[21] H. Zhou, H.-F. Chai, and M.-L. Qiu, ``Fraud detection within bankcard enrollment on mobile device based payment using machine learning,'' Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 15371545, Dec. 2018, doi: 10.1631/FITEE.1800580.

[22] S. Makki, Z. Assaghir,Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, ``An experimental study with imbalanced classication approaches for credit card fraud detection,'' IEEE Access, vol. 7, pp. 9301093022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[23] I. Matloob, S. A. Khan, and H. U. Rahman, ``Sequence mining and prediction-based healthcare fraud detection methodology,'' IEEE Access, vol. 8, pp. 143256143273, 2020, doi: 10.1109/ACCESS.2020.3013962.

[24] I. Mekterovi¢, M. Karan, D. Pintar, and L. Brki¢, ``Credit card fraud detection in card-not-present

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434

transactions: Where to invest?" Appl. Sci., vol. 11, no. 15, p. 6766, Jul. 2021, doi: 10.3390/app11156766.

[25] D. Molina, A. LaTorre, and F. Herrera, ``SHADE with iterative local search for large-scale global optimization," in Proc. IEEE Congr. Evol. Comput. (CEC), Jul. 2018, pp. 18, doi: 10.1109/CEC.2018.8477755.

[26] M. Muhsin, M. Kardoyo, S. Arief, A. Nurkhin, and H. Pramusinto, ``An analyis of student's academic fraud behavior," in Proc. Int. Conf. Learn. Innov. (ICLI), Malang, Indonesia, 2018, pp. 3438, doi: 10.2991/icli-17.2018.7.

[27] H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, ``Credit card fraud detection based on machine and deep learning," in Proc. 11th Int. Conf. Inf. Commun. Syst. (ICICS), Apr. 2020, pp. 204208, doi: 10.1109/ICICS49469.2020.239524.

[28] A. Pumsirirat and L. Yan, ``Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 1, pp. 1825, 2018, doi: 10.14569/IJACSA.2018.090103.

[29] P. Raghavan and N. E. Gayar, ``Fraud detection using machine learning and deep learning," in Proc. Int. Conf. Comput. Intell. Knowl. Economy (ICCIKE), Dec. 2019, pp. 334339, doi: 10.1109/ICCIKE47802.2019.9004231.

[30] M. Ramzan, A. Abid, H. U. Khan, S. M. Awan, A. Ismail, M. Ahmed, M. Ilyas, and A. Mahmood, ``A review on State-of-the-Art violence detection techniques," IEEE Access, vol. 7, pp. 107560107575, 2019, doi:10.1109/ACCESS.2019.2932114.

[31] M. Ramzan, H. U. Khan, S. M. Awan, A. Ismail, M. Ilyas, and A. Mahmood, ``A survey on state-of-the-art drowsiness detection techniques," IEEE Access, vol. 7, pp. 6190461919, 2019, doi: 10.1109/ACCESS.2019.2914373.

[32] A. Rb and S. K. Kr, ``Credit card fraud detection using artificial neural network," Global Transitions Proc., vol. 2, no. 1, pp. 3541, Jun. 2021, doi: 10.1016/j.gltp.2021.01.006.

[33] N. F. Ryman-Tubb, P. Krause, and W. Garn, ``How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," Eng. Appl. Artif. Intell., vol. 76, pp. 130157, Nov. 2018, doi: 10.1016/j.engappai.2018.07.008.

[34] I. Sadgali, N. Sael, and F. Benabbou, ``Adaptive model for credit card fraud detection," Int. J. Interact. Mobile Technol., vol. 14, no. 3, p. 54, Feb. 2020, doi: 10.3991/ijim.v14i03.11763.

[35] Y. Sahin and E. Duman, ``Detecting credit card fraud by ANN and logistic regression," in Proc. Int. Symp. Innov. Intell. Syst. Appl., Jun. 2011, pp. 315319, doi: 10.1109/INISTA.2011.5946108.

[36] I. Sohony, R. Pratap, and U. Nambiar, ``Ensemble learning for credit card fraud detection," in Proc. ACM India Joint Int. Conf. Data Sci. Manage. Data, Jan. 2018, pp. 289294, doi: 10.1145/3152494.3156815.

[37] B. Stojanovi¢, J. Boºi¢, K. Hofer-Schmitz, K. Nahrgang, A. Weber, A. Badii, M. Sundaram, E. Jordan, and J. Runevic, ``Follow the trail: Machine learning for fraud detection in fintech applications," Sensors, vol. 21, no. 5, p. 1594, Feb. 2021, doi: 10.3390/s21051594.

[38] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. Alemi, ``Inception-v4, inception-ResNet and the impact of residual connections on learning," 2016, arXiv:1602.07261.

[39] H. Tingfei, C. Guangquan, and H. Kuihua, ``Using variational auto encoding in credit card fraud detection," IEEE Access, vol. 8, pp. 149841149853, 2020, doi: 10.1109/ACCESS.2020.3015600.

[40] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, ``Credit card fraud detectionmachine learning methods," in Proc. 18th Int. Symp. INFOTEH-JAHORINA (INFOTEH), Mar. 2019, pp. 15, doi: 10.1109/INFOTEH.2019.8717766.

[41] S. Warghade, S. Desai, and V. Patil, ``Credit card fraud detection from imbalanced dataset using machine learning algorithm," Int. J. Comput. Trends Technol., vol. 68, no. 3, pp. 2228, Mar. 2020, doi: 10.14445/22312803/IJCTT-V68I3P105.

[42] N. Youse, M. Alaghband, and I. Garibay, ``A comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection," 2019, arXiv:1912.02629.

[43] X. Zhang, Y. Han, W. Xu, and Q. Wang, ``HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture," Inf. Sci., vol. 557, pp. 302316, May 2021, doi:10.1016/j.ins.2019.05.023.F

[44] H. A. El Bour, Y. Oubrahim, M. Y. Ghoumari, and M. Azzouazi, "Using isolation forest in anomaly detection: The case of credit card transactions," Periodicals Eng. Natural Sci., vol. 6, no. 2, pp. 394–400, 2018.

[45] A. Jog and A. A. Chandavale, "Implementation of credit card fraud detection system with concept drifts adaptation," in Proc. ICICC, Singapore, 2018, pp. 467–477.

[46] 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.

[47] F. Carcillo, Y.-A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," Inf. Sci., to be published.

[48] F. Carcillo, A. D. Pozzolo, Y.-A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, "SCARFF: A scalable framework for streaming credit card fraud detection with spark," Inf. Fusion, vol. 41, pp. 182–194, May 2018.

[49] R. Saia and S. Carta, "A frequency-domain-based pattern mining for credit card fraud detection," in Proc. 2nd Int. Conf. Internet Things, Big Data Secur., 2017, pp. 386–391.

[50] S. Yuan, X. Wu, J. Li, and A. Lu, "Spectrum-based deep neural networks for fraud detection," in Proc. ACM Conf. Inf. Knowl. Manage. (CIKM), 2017, pp. 2419–2422

DOI: https://doi.org/10.62647/IJITCE2025V13I2sPP425-434