An Intelligent Machine Learning Framework for Credit Card Fraud Detection

[1]Shantanu Deshmukh, [2]Shahjan khan, [3]Adarsh Paul
[1]Research scholar, Oriental Institute of Science and technology
Email ID - shantanudeshmukh3516@gmail.com
[2]Oriental Institute of Science and technology
Email ID - shahjankhan119@gmail.com
[3]Oriental College of Technology
Email ID - pauladarsh91@gmail.com

Abstract-Credit card fraud refers to the unauthorized use of an individual's credit card or the theft of card-related information to obtain financial benefits. Fraudulent activities take multiple forms, including counterfeit card fraud, card-not-present fraud, identity theft, and skimming attacks. With the rapid growth of online transactions and digital payment systems, credit card fraud has become a major concern for banks, financial institutions, and consumers worldwide. Traditional fraud detection techniques are often inadequate in handling the complexity, scale, and evolving nature of modern fraud patterns. In recent years, there has been significant interest in applying machine learning techniques to credit card fraud detection due to their ability to analyze large volumes of transaction data and identify hidden patterns associated with fraudulent behavior. Credit card fraud results in substantial financial losses for individuals and organizations, increases operational costs for banks, and undermines trust in the financial system. Victims may suffer not only monetary losses but also emotional distress and long-term damage to their credit records. Therefore, effective and intelligent fraud detection systems are essential to minimize unauthorized transactions, protect customer assets, and ensure the stability and reliability of financial services.

Keywords-Credit Card Fraud**,** Fraud Detection**,** Financial Transactions**,** Machine Learning**,** Card-Not-Present Fraud, Identity Theft**,** Skimming Attacks

INTRODUCTION

Credit card fraud involves using someone's credit card or stealing its information to get money [1]. This can involve various fraudulent activities, including: Counterfeit card fraud: Fraudsters make fake credit cardsby stealing credit card information [2]. This is followed by creating fake card numbers and PINs using the stolen data. Card-not-present fraud refers to stolen credit card data used for online or telephone purchases without the card being physically there [3]. Other categories of credit card fraud are identity theft, where one's details are stolen to create new credit card accounts, and skimming credit card fraud, where criminals use equipment installed on legit card readers to obtain credit card information .There has been tremendous interest in the machine learning approach towards recognizing credit card fraud detection. The issue of credit card fraud among banks is a growing concern. Credit card fraud leads to financial losses for individual card owners, banks, or companies that pay forunauthorised purchases [4]. Credit card fraud can cause aloss of faith and trust in the banking system, which may decrease consumer spending and economic instabilities. Credit card fraud can have financial and personal implications. Credit

card fraud victims can face various damages in terms of financial issues and confront the costs of non-authorized transfers. Individuals can be distressed emotionally and experience damage to credit records [5].The other financial cost relates in a way that includes covering such issues as paying back funds when credit card fraud happens and implementing a system to safeguard against further malpractices. Credit card fraud affects society since the victims are not only those directly hurt by the crime. Moreover, the ripple impact of credit card fraud impacts the broader economy and society. These days, a concept called "digitization" has a huge impact on the younger population. Having this digital literacy understanding has far-reaching effects on many economic areas, including banking, finance, insurance, and more. In order to provide their customers with first-rate services and future income opportunities, the Indian banking sector should put digitization at the top of its priority list. This is due to the fact that digitalization is vital to financial inclusion.The majority of consumers now use online banking as their default method of transferring funds. Through the use of internet banking, an increasing number of individuals are able to pay for a variety of expenses, including but not limited to insurance premiums, travelling tickets and utility bills (including power, water, and property taxes), online purchases etc.The efficacy of internet banking has been progressively increasing. An important negative aspect of this expansion is the rise of deceitful practices.The concept of online banking, more commonly known as "e-banking" or "Internet banking," grew rapidly in the years leading up to the present day[6].The majority of consumers now use online banking as their primary method for transferring funds.

Figure. 1. Statistics Worldwide Card Frauds [3]

Through internet banking, an increasing number of individuals are able to pay for a wide range of expenses, including insurance premiums, travel tickets, utility bills such as electricity, water, and property taxes, as well as online purchases. The efficiency and convenience of internet banking have steadily increased over time. However, a significant negative consequence of this expansion is the rise in fraudulent activities [7].The concept of online banking, commonly referred to as e-banking or internet banking, has grown

rapidly in recent years due to advancements in digital technologies and widespread internet access .While these developments have enhanced customer convenience and accessibility, they have also created new security challenges, making financial systems more vulnerable to cyber threats and fraudulent transactions.

Credit card firms play a significant role in the contemporary digital landscape. American Express, Citibank, and Capital One are prominent credit card firms leading the market

Credit card firms play a significant role in the contemporary digital landscape. American Express, Citibank, and Capital One are prominent credit card firms leading the market. Standing in the realm of Big Data. Investigating the purchasing history of card users is nearly impossible. In response to the escalating volume of transactional data, leading firms are using Hadoop and machine learning methodologies to address data storage and scalability challenges. Approximately $35 billion in firms have used the Apache Hadoop framework for data storage, facilitating over $1.5 trillion in annual transactions, which constitutes roughly one-fourth of all credit card transactions. The most recent report by Nilson indicates that global fraud losses amounted to $27.85 billion in 2018 and are projected to escalate to $35.67 billion by 2025, as illustrated in Fig. 1

In this digital era everyone has use online banking services and digital card payments. Banks have newly developed electronic banking services and developed various facility regarding financial transactions and services, which lets users control their accounts online. With internet banking, you can do a lot of various kinds of financial transactions [9]. A quantity of these is ATM withdrawal, direct deposits, electronic financial transfers (EFTs), automatic bill payments (ABPs), and more. But it's cheap, easy to use, and can be changed, which is not the case with traditional banking. The development of this better online banking system was slowed down by the risk and attacks of fraud data settling [10]. Hackers can get into online banking systems because of new hacking methods. There are now many more online application suppliers for both businesses and consumers. This has led to more scams and attacks. With this in mind, it's important to have robust ways to prove who you are when doing business online. As information and communication technologies have become more common, the requirement for strong cryptographic systems has grown.[11-12]

Digital Banking

One innovative industry is digital banking, sometimes known as electronic banking. Customers may manage their money from anywhere in the world thanks to the internet. Among the many developments handled by the electronic banking system are the following: the necessity of meeting customer demand for services at all times and in all places; the importance of a product's time to market; and the challenges associated with integrating bank offices.The digital banking system permits the customers for accessing their banking account, demand a current account statement, reorder checks, product information, observation of current bank rates, and accessing latest transactions. Along with this, various banks, namely Citibank, Fleet Financial Group, Royal Bank of Canada, Chevy Chase, Bank of America, Mellon Bank, KeyCorp, Michigan National Bank, Bank One, Bank, Comerica, First Bank Systems, and so on are presently providing these services. The electronic banking system is normally considered as an expansion of

present banking system. Plus, it's called Internet banking because any customer with a computer and a web browser can access their bank's website and do a variety of necessary financial tasks there. Plus, digital banking makes use of the bank's federal dataset. With internet banking, you can do all your banking whenever and wherever you like because it knows no geographical boundaries [13].

- **Credit Card Fraud:** Offline and online credit card fraud are the two main categories.
- Offline fraud is perpetrated by making use of a counterfeit or stolen physical card at a variety of establishments.
- On-line fraud commits the crime while the cardholder is not present, over the phone, online, or while shopping.
- Telecommunication Fraud: in the absence of the cardholder, when transacted over the phone, online, or during a shopping trip.

[14] Used a powerful generalized response model to predict management fraud. The "probit and logit" methods are a part of the model. Credit cards and their many varieties are defined at the outset of this paper, which then moves on to discuss relevant research and potential methods and models for identifying legitimate and fraudulent purchases.

The Act Of Entering Without Warrant Or Invitation; That Means “Potential Possibility Of Unauthorized Attempt To Access Information, Manipulate Information Purposefully. Intruders May Be From Any Environment, An Outsider (Or Hacker) And An Insider Who Knos The Layout Of The System.

Computer intrusion can be classified into three categories: misuse intrusions, network intrusions and host intrusions. Misuse intrusions analyze the information gather and compare it to large databases of attack signatures. Network intrusions, individual packets flowing through a network are analyzed. Passive intrusions, detects a potential security breach, logs the information and signals an alert.

Bankruptcy Fraud: This column focuses on bankruptcy fraud. Bankruptcy fraud means using a credit card while being absent. Bankruptcy fraud is one of the most complicated types of fraud to predict. Some methods or techniques may help in fraud prevention. The bank will send its users/customers an order to pay. However, the users will be recognized as being in a state of personal bankruptcy and not able to recover their unwanted loans. The bank will have to cover the losses itself. One of the possible ways to prevent bankruptcy fraud is by doing a pre-check with credit bureau in order to be informed about the past banking history of its customers. [15] presented a model to forecast personal bankruptcy among users of credit card.

Theft Fraud/ Counterfeit Fraud: In this section, we focus on theft and counterfeit fraud, which are related to one other. Theft fraud refers using a card that is not yours. As soon as the owner give some feedback and contact the bank, the bank will take measures to check the thief as early as possible. Likewise, counterfeit fraud occurs when the credit card is used remotely; where only the credit card details are needed. Firstly, use of your copied card number and codes via various web-sites, where no signature or physical cards are required. [6] although in European E-commerce seems to be quite low, at only 0.83 percent along with the average charge-back ratio, significant concerns are notified in detailed analysis. For the listed credit card, the customers are contacted and if they do not react within certain time limit than the card is blocked.

Application Fraud: When someone applies for a credit card with false information that is

termed as application fraud. For detecting application fraud, two different situations have to be classified. When applications come from a same user with the same details, that is called duplicates, and when applications come from different individuals with similar details, that is termed as identity fraudsters. [7]describes application fraud as "demonstration of identity crime, occurs when application form(s) contain possible, and synthetic (identity fraud), or real but also stolen identity information (identity theft)." In most of the banks, eligibility for a credit card, applicants need to complete an application form. Application form is mandatory except for social fields. The bank would also ask for certain details as contact details, such as e-mail address, mobile phone number and land-line number. Confidential information will be the password.[16]

Behavioral Fraud: Behavioral fraud occurs when sales are made on a „cardholder present" basis and details of legitimate cards have been obtained fraudulent basis.

Credit Card Fraud Detection

Issues with credit cards, both theoretical and practical, are discussed in this section.

Credit Card: They can buy things online without actually having the cash on hand through the use a credit card. The use of a credit card streamlines the process of automatically extending credit to consumers. Almost all credit cards now include a unique identifier that speeds up online purchases.

Fraud: Any dishonesty perpetrated with the aim to deceive another person or entity for one's own benefit or harm is considered fraudulent. The concept of fraud is defined differently in different legal systems. Deceit is both a criminal offense and a breach of civil law. One typical goal of fraud is to defraud individuals or organizations of their money.

Security in Banking

There are several potential threats that could compromise these three security pillars, including malicious actors, technological issues, accidents, and natural calamities. Ensuring the privacy of information entails limiting its visibility to authorized users exclusively, while prohibiting unauthorized individuals from accessing it. Also, only people who have permission will be able to see the information you give, which keeps it private. To identify people and protect sensitive data, passwords and user IDs are employed as authentication methods. Also, more ways to regulate access are put in place to protect privacy. For example, the data system limits the resources that each identifiable user can utilize..Along with this, the most important thing for secrecy is protection against spam, malware, other assaults, spyware, etc. [17]

The enormous challenge of security is inherent in any online financial service. When they first try to take someone's money, thieves follow a very complicated and dangerous procedure. Although, if any card and transaction information received by any other person as well as specific pieces of personal information about customers, so the received person easily steal funds from their online bank accounts. According to [18], physical, geographical, informational, and communicative privacy are the four main types. Most of the time, when we speak about "people's ability to govern their own data," what we mean is that they can retain the privacy of their online identities. The lack of control over acquired and used personal data constitutes a violation of people's privacy. The foundational principles of information security are confidentiality, availability, and integrity.

Generally speaking, the Certified Internal Auditor (CIA) standard is followed by those who verify the safety of an online store's computer systems.

Types of Credit Card Fraud

Studies of credit card fraud cases show that these five forms of fraud are the most widespread.

- Forgeries of commercial credit
- Card lost
- Cardholder-Not-Present (CNP)
- Account Takeover
- Phishing

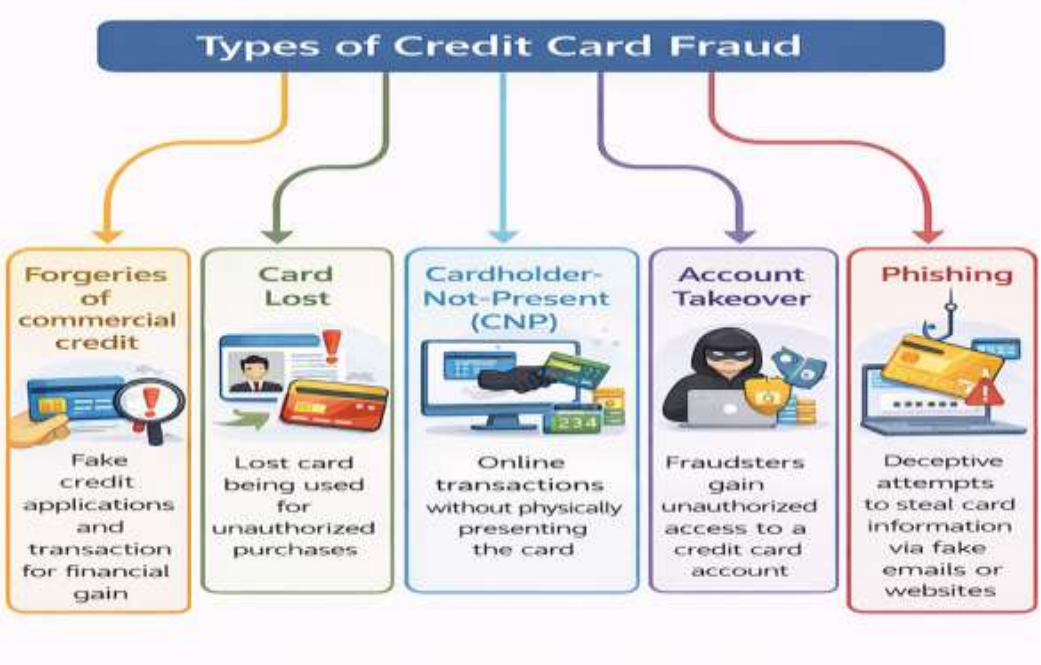

Figure 2 Types of Credit Card Fraud [10]

Counterfeit Credit Cards

One of the worst forms of credit card theft is using stolen card information to make counterfeit cards. In their insatiable need for novelty, fraudsters are always thinking of new ways to create fake cards. Illegal methods abound for creating fraudulent and counterfeit cards, including removing the magnetic strip, altering the card's data, skimming, collaborating with businesses, and creating new cards.[19]

Cardholder-Not-Present (CNP)

The most common way to commit this type of credit card fraud is to get duplicate card data and then use that data along with fake personal information to make CNP purchases. You can only use a CNP to buy things online. In this kind of fraud, the cardholder and the card are not physically present. There are many methods to make a transaction, such via the phone, the internet, the mail, or a fax, therefore fraud can happen in a lot of different ways. Because businesses can't check the card or figure out who the cardholder is, it's hard to tell who the user is and who they really are in these transactions.

Account Takeover

In the context of identity theft, phishing is one kind of fraud. Common entry points for this kind of assault include spam emails or windows that pop up unexpectedly. Phishing attacks happen

when an unscrupulous individual sends out a deluge of emails that look like they came from a legitimate company or website. The message specifically requests that the recipient provide sensitive information (such as a credit card number) to the company. These businesses may be able to use the data to their advantage if they blame a database crash.As part of this scheme, the con artist may include a link in the email that appears to be coming from a legitimate-looking website, but is actually a scam site.[20]

LITERATURE REVIEW

Recent advances in credit card fraud detection have leveraged a variety of novel data augmentation, anomaly detection, and feature engineering techniques to address challenges such as class imbalance, evolving fraud patterns, and high-cardinality transaction features. For example, [21] introduced K CGAN, a generative augmentation model that outperforms traditional oversampling methods—such as B SMOTE and SMOTE—in both F1 score and overall accuracy, while also achieving top precision and recall on a benchmark fraud dataset. In the unsupervised domain, developed UAAD FDNet, which combines autoencoders with feature attention and a GAN to detect outlier transactions; when tested on both Kaggle and IEEE CIS datasets, this framework demonstrated superior capabilities in identifying novel fraudulent behaviors. tackled Card Not Present fraud by applying dimensionality reduction methods (PCA, SVD, t SNE) followed by logistic regression, producing an effective detection and prevention pipeline in a Python implementation.

Recent literature shows that ensemble learning techniques, including bagging and boosting, significantly improve fraud detection performance by reducing variance and handling class imbalance more effectively. Studies have also demonstrated that deep learning models, such as Artificial Neural Networks, Convolutional Neural Networks, and Recurrent Neural Networks, are capable of automatically extracting complex features from transaction data and identifying subtle fraud patterns. Additionally, anomaly detection methods have been widely used to detect rare and unusual transaction behaviors, thereby minimizing false negatives.

Several authors have emphasized the importance of incorporating contextual and auxiliary information, such as user behavior, geographic location, and transaction history, to enhance fraud detection accuracy. Despite these advancements, challenges such as data imbalance, model interpretability, and real-time deployment remain open research issues. The existing literature indicates a strong need for integrated frameworks that combine ensemble learning, deep learning, and explainable AI techniques to develop reliable and practical fraud detection systems for modern financial environments.[21]

The rapid growth of online and internet banking has significantly transformed the way financial transactions are carried out, offering greater convenience, speed, and accessibility to consumers. However, this digital transformation has also led to a substantial increase in credit card fraud and other financial cybercrimes. Traditional rule-based fraud detection methods are increasingly ineffective due to their limited adaptability and high false-positive rates in the presence of evolving fraud patterns. This study emphasized the importance of intelligent fraud detection systems based on machine learning and deep learning techniques. The analysis

demonstrated that data-driven models can effectively learn complex transaction patterns and improve the detection of fraudulent activities. Ensemble learning approaches further enhanced detection accuracy by combining the strengths of multiple classifiers, while deep learning models showed strong potential in capturing non-linear and temporal relationships within transaction data. the study concludes that robust, adaptive, and scalable fraud detection frameworks are essential to protect financial institutions and customers, maintain trust in digital banking systems, and support secure real-time financial transactions.[22]

Table:1 Literature Review on Credit Card Fraud Detection

Author(s) & Year	Dataset	Methodology / Models Used	Key Technique / Contribution	Performance / Findings
[21]	European credit card dataset	Ensemble ML (Bagging, Boosting, RF, SVM, KNN)	SMOTE + under-sampling to handle imbalance	Achieved superior accuracy, precision, recall, and F1-score
[22]	European cardholder dataset	Compact Data Learning (CDL)	Feature reduction without loss of accuracy	Outperformed traditional ML and feature reduction methods
[23]	Kaggle credit card dataset	Meta-Heuristic Optimization (MHO)	Feature selection using 15 MHO methods	97% accuracy with 90% feature reduction
[24]	Real-world transaction data	Hybrid ML models (Adaboost + LGBM)	Hybrid learning approach	Adaboost + LGBM achieved best detection accuracy
[25]	Credit card dataset	Text2IMG + CNN + Coarse-KNN	Image-based representation of transactions	Achieved 99.87% accuracy

Table 2 how data imbalance is addressed and the advancements in machine learning techniques:[27]

Method/Technique	Description	Advantages	Disadvantages	Applications
Random Oversampling	Duplicating samples from the minority class to balance class distribution.	Simple to implement, can improve model performance on imbalanced datasets.	Can lead to overfitting due to duplicated samples, may not generalize well.	Fraud detection, medical diagnosis (imbalanced classes).
Random Undersampling	Randomly removing samples from the majority class to balance the	Reduces the size of the dataset, reducing training time.	Loss of potentially useful data from the majority class, may lead	Customer churn prediction, spam detection.

	dataset.		to underfitting.	
SMOTE (Synthetic Minority Over-sampling Technique)	Generates synthetic samples for the minority class based on nearest neighbors.	Creates diverse synthetic samples, reduces overfitting compared to random oversampling.	May create unrealistic samples or noise if not tuned properly.	Credit card fraud detection, rare event prediction.
ADASYN (Adaptive Synthetic Sampling)	A variation of SMOTE that focuses on generating synthetic samples for difficult-to-classify instances.	Addresses class imbalance more effectively by focusing on harder examples.	Computationally expensive, can generate noisy or redundant samples.	Intrusion detection, medical diagnosis.
Class Weight Adjustment (in Algorithms like SVC, Logistic Regression)	Assigns different weights to each class during model training to penalize misclassifications of the minority class.	Prevents the model from biasing toward the majority class, easy to implement.	Requires careful tuning of the weights to avoid overemphasizing the minority class.	Imbalanced binary classification tasks.
Ensemble Methods (Bagging, Boosting, Stacking)	Combining multiple weak models to form a strong predictive model, with techniques like **Bagging**, **Boosting**, and **Stacking**.	Boosts performance by leveraging multiple weak models, helps in reducing bias and variance.	Can be computationally expensive and harder to interpret.	Text classification, fraud detection.
Anomaly Detection Techniques	Treats the minority class as anomalies and focuses on detecting them as outliers.	Effective for highly imbalanced datasets where minority class is rare.	May not be suitable for cases where the minority class isn't well-defined as an anomaly.	Fraud detection, network intrusion detection.
Balanced Random Forest	A variant of Random Forest that adjusts for	Good at handling class imbalance,	Can still be prone to overfitting if not	Classification tasks with imbalanced

	imbalances by modifying how trees are constructed.	reduces overfitting by adjusting class distribution in each tree.	tuned correctly.	classes.
Cost-sensitive Learning	Modifies learning algorithms to take the cost of misclassifying different classes into account.	More control over class misclassification cost, improves focus on minority class.	Requires domain knowledge to assign appropriate costs, may not be suitable for all tasks.	Risk prediction, financial fraud detection.
Transfer Learning	Leverages pre-trained models on a large dataset to help with imbalanced data tasks.	Can reduce the need for large imbalanced datasets, can generalize better from transfer learning.	May require large pre-trained models and significant computational resources.	Image classification, NLP tasks with imbalanced labels.

CONCLUSION

The research papers reviewed collectively emphasize the growing concern of credit card fraud in an era of increasing online transactions and technological advancements. As fraud detection systems face the challenge of imbalanced datasets, with fraudulent transactions being significantly fewer than legitimate ones, various innovative techniques have been explored to enhance detection accuracy and reduce the impact of data imbalance.Most studies reported significant improvements over traditional methods. For example, ensemble models outperformed individual classifiers in various metrics, including precision, recall, accuracy, and F1-score. Similarly, data augmentation strategies like K-CGAN and SMOTE demonstrated superior results in precision and recall, with K-CGAN specifically showing the best performance in terms of F1 score and accuracy.Many of the studies highlighted the importance of effective feature selection and feature reduction techniques. Meta-heuristic optimization methods were frequently used to identify the most critical features, leading to models that not only performed better but also required fewer resources for training.The studies also emphasize the need for continuous innovation and adaptability in fraud detection systems. As fraud tactics evolve, so too must the techniques used to detect them. The ongoing development of hybrid machine learning models and the exploration of novel data augmentation and feature selection methods will likely be key to future advancements in this field.

REFERENCE

1. Mbama C I and Ezepue P O, “Digital banking, customer experience and bank financial performance”, International Journal of Bank Marketing, April 2018.

2. AleksandarLukic, “Benefits and Security Threats in Electronic Banking International”, Journal of Managerial Studies and Research, vol.3, no.6, pp.44-47, 2015.
3. Revathi P, “Digital Banking Challenges and Opportunities in India”, EPRA International Journal of Economic and Business Review, vol.7, no.12, pp.20-3, 2019.
4. Nayak R, “A Conceptual Study on Digitalization of Banking-Issues and Challenges in Rural India”, International Journal of Management, IT and Engineering, vol.8, no.6, pp.186-91, 2018.
5. Dagada R, “Digital banking security, risk and credibility concerns in South Africa”, In proceedings of The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic, 2013.
6. Achituve I, Kraus S, Goldberger J, “Interpretable Online Banking Fraud Detection Based on Hierarchical Attention Mechanism”, In proceedings of 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP), pp.1-6, October 2019.
7. Wei W, Li J, Cao L, Ou Y, Chen J, “Effective detection of sophisticated online banking fraud on extremely imbalanced data”, World Wide Web, vol.16, no.4, pp.449-75, July 2013
8. Singh P and Singh M, “Fraud detection by monitoring customer behavior and ctivities”, International Journal of Computer Applications, vol.111, pp.11, January 2015.
9. Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F, “Using generative adversarial networks for improving classification effectiveness in credit card fraud detection”, Information Sciences, vol.479, pp.448-55, April 2019.
10. Kazemi, Z., and Zarrabi, H., "Using deep networks for fraud detection in the credit card transactions," In proceedings of 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), IEEE, 2017
11. Carcillo F, Le Borgne Y A, Caelen O, Kessaci Y, Oblé F, Bontempi G, “Combining unsupervised and supervised learning in credit card fraud detection”, Information Sciences, May 2019.
12. Zhou, H., Chai, H., and Qiu, M, “ Fraud detection within bankcard enrollment on mobile device based payment using machine learning,” Frontiers of Information Technology & Electronic Engineering, vol.19, no.12, pp.1537–1545, 2018.
13. Bahnsen, A.C., Stojanovic, A., Aouada, D. and Ottersten, B.,”Cost sensitive credit card fraud detection using Bayes minimum risk”, In proceedings of 12th international conference on machine learning and applications, vol. 1, pp. 333-338, December 2013.
14. A.D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, Credit Card Fraud Detection : A Realistic

Modeling and a Novel Learning Strategy. 29(8) (2018) 3784–3797

15. A. Dal Pozzolo, O. Caelen, Y.A. Le Borgne, S. Waterschoot, G. Bontempi, Learned lessons in credit card fraud detection from a practitioner perspective, Expert Syst. Appl. 41 (10) (2014) 4915–4928.
16. G. Bontempi, Reproducible machine learning for credit card fraud detection - practical machine learning for credit card fraud detection - practical handbookforeword. May, 2021.
17. Kazemi, Z., and Zarrabi, H., "Using deep networks for fraud detection in the credit card transactions," In proceedings of 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), IEEE, 2017
18. Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., and Pan, S., "Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network," In proceedings of 13th International Conference on Computer Science & Education (ICCSE), 2018.
19. Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., and Pan, S., "Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network," In proceedings of 13th International Conference on Computer Science & Education (ICCSE), 2018.
20. Nayak R, "A Conceptual Study on Digitalization of Banking-Issues and Challenges in Rural India", International Journal of Management, IT and Engineering, vol.8, no.6, pp.186-91, 2018.
21. Dagada R, "Digital banking security, risk and credibility concerns in South Africa", In proceedings of The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic, 2013.
22. Esraa Faisal Malik,Khai Wah Khaw,Bahari Belaton,Bahari Belaton,Wai Peng Wong,XinYing Chew (2022) "Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture" 2022, 10(9), 1480; https://doi.org/10.3390/math10091480, 28 April 2022
23. Igor Mekterović,Mladen Karan,DamirPintar,Ljiljana Brkić (2021) "Credit Card Fraud Detection in Card-Not-Present Transactions: Where to Invest" 021, 11(15), 6766; https://doi.org/10.3390/app11156766, 23 July 2021
24. EmilijaStrelcenia,SimantPrakoonwit (2023) "Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation" 2023, 4(1), 172-198; https://doi.org/10.3390/ai4010008, 31 January 2023
25. Abdullah Alharbi,Majid Alshammari, of ojime Dominic Okon, Amerah Alabrah,Hafiz Tayyab Rauf ,Hashem Alyami, Talha Meraj (2022) "A Novel text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach" 2022, 11(5), 756; https://doi.org/10.3390/electronics11050756, 1 March 2022.