Volume 10, Issue 4, April – 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges

Swapnil Jagannath Wawge[1]

[1]Sr Mgr, Engineering Lehi, Utah, USA

Publication Date: 2025/05/13

Abstract: Credit card usage is essential in the current economic climate. It has become a necessary component of domestic, commercial, and international operations. Even though there are many advantages to using credit cards when done properly and sensibly, fraudulent activity can result in serious credit and financial harm. Credit card fraud is becoming more of an issue in the financial services industry because more unauthorized payments lead to significant losses. Because of the high amount of transactions and changing fraud patterns, traditional rule-based fraud detection techniques are no longer adequate. Machine learning (ML) techniques provide viable ways to analyze trends and anomalies in order to detect fraudulent transactions. This research looks at a number of machines learning methods, including both supervised and unsupervised training strategies, emphasizing their accuracy, effectiveness, and drawbacks. In order to increase detection rates, the study also looks at assessment metrics, data imbalance problems, and new hybrid models. Lastly, important issues including privacy issues, limitations on real-time detection, and changing fraud tactics are covered, highlighting the necessity of flexible and expandable fraud detection systems.

Keywords: *Credit Card Fraud Detection, Machine Learning, Technique, Challenges in Credit Card Fraud.*

How to Cite: Swapnil Jagannath Wawge (2025). A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges. *International Journal of Innovative Science and Research Technology*, 10(4), 3345-3352. https://doi.org/10.38124/ijisrt/25apr1813

I. INTRODUCTION

The moment a credit card is used unlawfully and without authorization from somebody other than the cardholder, it is known as credit card fraud. Financial companies and customers often suffer losses as a result of this[1]. It includes situations in which a malevolent actor utilizes someone else's credit card details that are not known to the customer or the originating that issued it or approval. Therefore, fraud detection is a crucial duty that entails ongoing user activity monitoring to detect, stop, and lessen questionable behaviors, such as fraud, intrusion, and defaulting[2].

The need to protect transactions and stop fraudulent activity has never been more important due to global credit card usage dramatic increase. Approximately 70% of the 2.8 billion credit card users worldwide in 2019 had at least one card, according to the 2021 Credit Card Statistics[3]. In the United States alone, there were 393,207 credit card fraud reports in 2020, compared to 271,927 in 2019, a 44.7% increase. Identity theft, in which a false account is formed in someone else's name, is one especially concerning form of fraud; this sort of incidence increased by 48% between 2019 and 2020.

The mismatch in transaction data is among the most significant barriers to identifying credit card fraud. Because fraudulent transactions are so few in comparison to legal ones, the dataset is highly skewed. This disparity may lead to skewed model performance and inadequate fraud detection. Investigators have used a number of data-balancing techniques, including SMOTE, insufficient sampling, and the technique of overs to address this issue. Despite the potential of these methods, a thorough assessment of their accuracy, effectiveness, and practicality is still required. The dynamic nature of financial fraud makes it necessary to employ flexible systems that can identify new patterns and anomalies[4].

One of the most potent supervised learning algorithms among the ML approaches employed is the SVM. Applications for it are numerous and include public safety, credit scoring, and image recognition[5]. Because SVMs can differentiate between unauthorized and authentic interactions and resolve either linear and nonlinear classification of binary issues. In a high-dimensional field, they identify the best hyperplane to divide data points. SVM can handle binary categorization that is both linear and asymmetric issues. Neural networks, which were the foundation for subsequent DL approaches, were utilized in early credit card fraud detection technologies[6]. The emphasis has gradually moved to assessing various ML models in terms of their precision, accuracy, computational efficiency, ability to adjust to the constantly evolving patterns

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

of fraudulent activity, accuracy in handling unbalanced data, real-time detection, and adaptive learning.

➢ *Structure of the Paper*

This research paper is organized as follows: Section II delivers an impression of detecting credit card fraud. Section III ML technique based on credit cards Section IV provides credit card performance data, while Section V discusses the tasks modelled by credit card fraud. Section VI summarizes the body of research on the topic and offers suggestions for more study.

II. OVERVIEW OF CREDIT CARD FRAUD DETECTION

Fig 1 Credit Card Fraud Detection

The quantity and variety of credit card transactions are significant[7]. Based on their regions and currencies, the consumers' credit card usage demonstrates the vast range of fraudulent transactions. This issue has spurred me to come up with a technique that would make it possible to identify fraudulent transactions regardless of where they occur. Another multi-objective assignment is fraud detection. The digital hand in Figure 1 is trying to steal a credit card, signifying online credit card fraud or cyber theft.

Banks and additional economic organizations must always provide their customers with positive experiences and services. As a result, using user datasets for testing while maintaining service uptime and privacy is difficult. My passion brings me to the federated learning architecture for ensuring data privacy. Figure 2 shows the threat of credit card fraud. With an astounding 19% fraud rate, Ukraine leads the pack, closely followed by Indonesia (18.3%). The most dangerous nation after these two is Yugoslavia, with a rate of 17.8%. The United States has the greatest fraud rate, followed by Turkey (9%) and Malaysia (5.9%). Figure 2 does not include information on other nations where credit card fraud is less than 1%.

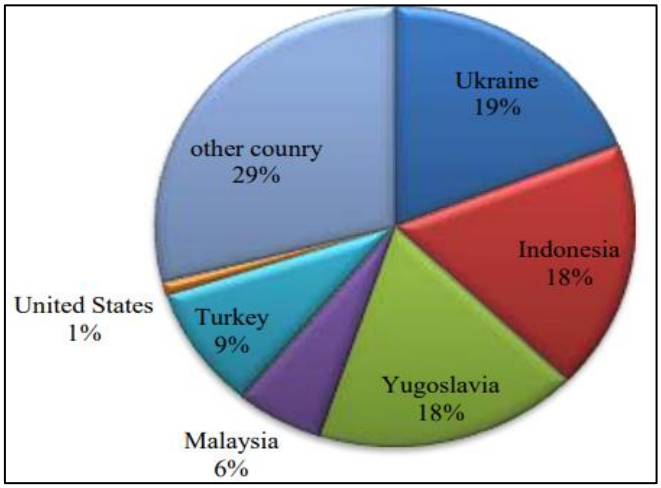

Fig 2 High-Risk Countries Fraud in Credit Card Threat

As technology advances, the number of individuals utilizing the www and doing business from home is increasing. Credit cards are used for the vast majority of these purchases. The implementation of fraud detection or mitigation is necessary to lower these financial losses. Fraud takes in different forms as technology develops quickly. Pattern matching, AI techniques, and various data mining and statistical methods have all been developed by researchers to identify fraudulent transactions. Numerous studies have proposed various ML and DL classifiers in recent years to identify fraudulent transactions.

➢ *Types of Credit Card Fraud*

There are several divisions that the main types of credit card fraud may fall under in Figure 3. These comprise both digital and physical ways that cards can be used without authorization:

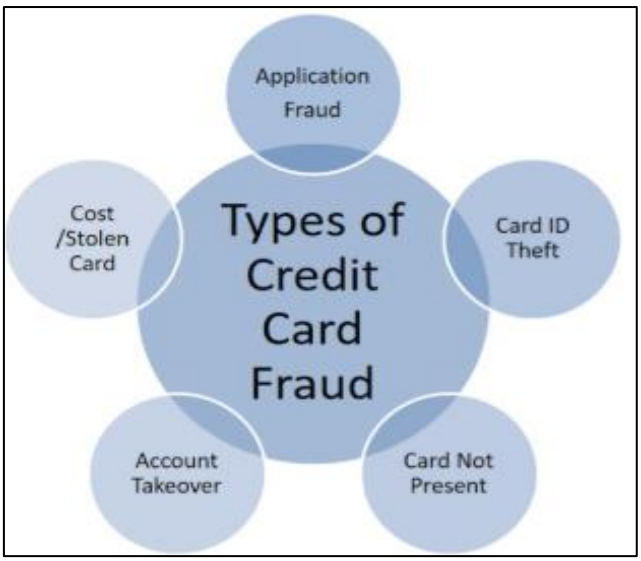

Fig 3 Types of Credit Card Fraud

- **Application fraud:** A fraudster gains access to an application system by stealing personal data, including a login and password, and fabricating an account[8]. Usually, identity theft is the cause of this.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

- **Electronic or manual credit card imprints:** The moment the scammer scans the information on the magnetic surface of the card. This data is very confidential, and if someone manages to obtain it, they might use it to commit fraud.
- **CNP (card not present):** The fraudster can use the card without being physically present as long as they know the account number and expiration date.
- **Counterfeit card Fraud:** A common way to try it is via skimming. All of the actual card's data is included on a fake magnetically swipe card. The phony card may be employed to make transactions and is completely functioning.
- **Lost and Stolen card fraud:** In the event that Fraudsters may obtain the card and use it to make purchases if the actual cardholder loses it. It is challenging to do this via machine since a pin number is required, but the fraudster finds online transactions to be rather easy.
- **Card ID theft:** This fraud and application fraud are comparable. When someone commits identity theft, they get the initial version card's information in order to use it or create a new account. The most difficult kind of scam to identify is this one.

➢ *Authentication Mechanism to Prevent Fraud*

Some of the most current and pertinent articles about user authentication. Generally speaking, the articles in this field belong to one of the categories listed below:

- Graphical password-based authentication systems, Personal Identification Numbers (PINs), and password-based authentication techniques include[9]. It recommends utilizing a novel method based on human body measures or activities, known as biometric-based methods, since this category of user authentication techniques is practical and easy to use, but they are extremely unsafe and Long-term memory constraints make people more inclined to use basic passwords.
- Physiological authentication and behavioral authentication are the two subcategories of biometric-based authentication techniques. The former discusses authentication methods that rely on physical attributes of the human body, such the face, finger, iris, voice, or retina. Physiological methods of authentication have some drawbacks and are not as effective as password-based methods.
- Among the most modern methods for user authentication schemes are combined authentication techniques. These methods take into account many of the previously listed criteria to improve the system's accuracy while preserving its usability.

III. MACHINE LEARNING TECHNIQUE FOR FRAUD DETECTION

A ML- based method for detecting credit card fraud was created by using combinations of models that combine the popular vote stargates and AdaBoost. They added 10% to 30% noise to their hybrid models to make them simpler to operate[10][11]. A respectable examination of the information gathered from a group with 30% greater noise, the different voting methods received a score of 0.942. ML algorithms are crucial for detecting credit card fraud because of their capacity to learn from data, recognize complicated patterns, and forecast credit card theft[12][13]. The algorithms mentioned above are examples of both supervised and unsupervised learning methods. The methodologies listed below are used in Credit Card Fraud Detection: RF, KNN, NB, DT, LR, SVM, and Tree-Augmented Naive Bayes (TAN). RF incorporates DT through the implementation of a tree-like interdependence framework for capturing feature correlations, TAN improves NB and lessens excessive fitting, and SVM uses the best hyperplane to classify data points[14][15]. These models contribute to strong fraud detection systems by providing a variety of methods for spotting and stopping fraudulent transactions.

➢ *Supervised Learning Approaches*

In supervised approaches[16], annotated instances Algorithms that categorize interactions as either legitimate or dishonest are built using data from both fraudulent and non-fraudulent business transactions. On the other hand, techniques that are unsupervised search for customers, user accounts, interactions, etc, that create questions because they deviate greatly from the majority of data. Anomaly identification or outlier detection is the process of identifying such unusual data.

- **Logistic regression:** The LR technique is a widely used method for binary classification[17] As an input of the sigmoid function, a simple combination of many characteristic values or explication information is usually accepted by the LR classification factors. A more precise definition of class 1 is an input that produces a result greater than 0.5[18]. However, if the output is smaller than 0, the matching input is in the 0 class.
- **Support vector machine:** SVM is a supervised ML method that could be used to perform categorization and regressive analyses. However, it is mostly applied to categorization issues.

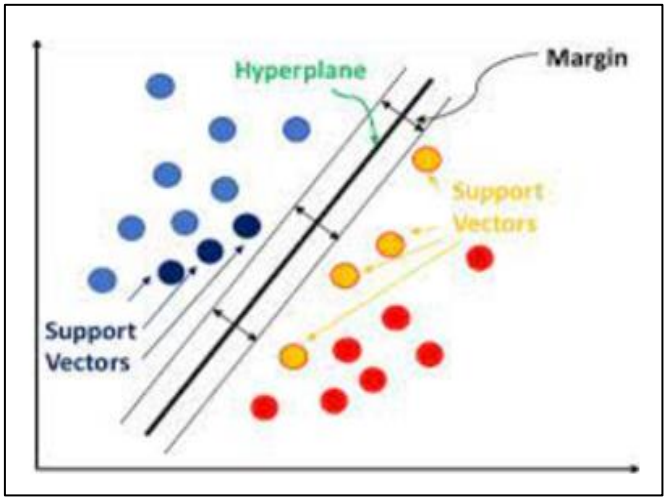

Fig 4 SVM Algorithm

In this Figure 4 SVM algorithm is classified as binary. Therefore, the transactions are either categorized as legitimate or fraudulent. This aids us in identifying users' unusual behavior.

➢ *Unsupervised Learning Approach*

Additionally, the field of fraud detection has included methods for unsupervised learning, include segmentation or

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

identifying outliers[19]. These methods don't require pre-made labels to examine the information about transactions for patterns and anomalies. Techniques that combine transactions that are similar might identify trends that can point to fraud[20]. In contrast, Algorithms for outlier identification can identify very atypical financial activities that can indicate fraud. Predictive modelling techniques and data analytics have proved very helpful in identifying fraud. Modelling methods such as RF and LR.

- **Clustering techniques (k-means):** The challenge of breaking down a given collection of items into meaningful subsets is addressed by clustering, an unsupervised data mining approach[21]. The clusters that emerge from this data segmentation must be homogenous and/or well-separated, with comparable items within one group and dissimilar ones within other groups.
- **Autoencoder for anomaly detection:** The first usage of autoencoder neural networks for identifying anomalies in WSNs for IoT uses[22]. A two-level strategy was implemented, with the second-level, computationally demanding learning activity taking place on the cloud level much less often than the first-level algorithm, which runs on sensor nodes.

➢ *Deep Learning Approach*

Data is used in DL, a branch of ML, to educate computers to do tasks[23]. The basic idea behind DL is that as we grow our neural networks and train them with fresh data, their performance keeps getting better.

- **Artificial Neural Network:** A collection of interconnected nodes created to mimic how the human brain works is called an ANN. Every node is connected to several other nodes in neighboring levels in a weighted manner. ANNs may be set up using hybrid, supervised, or unsupervised learning techniques.
- **Convolution neural network:** The CNN is a popular DL architecture that has recently been used to several CCFD models. It produces state-of-the-art results in image identification. It is composed of neurons that have biases and weights that can be learnt. After the convolutional and pooling layers have extracted features and down-sampled, respectively, the completely associated coatings convert their output to the CNN's final output[24]. This conversion gives an estimate of likelihood for every category (fraud or non-fraud) in an issue with classification such as CCFD.

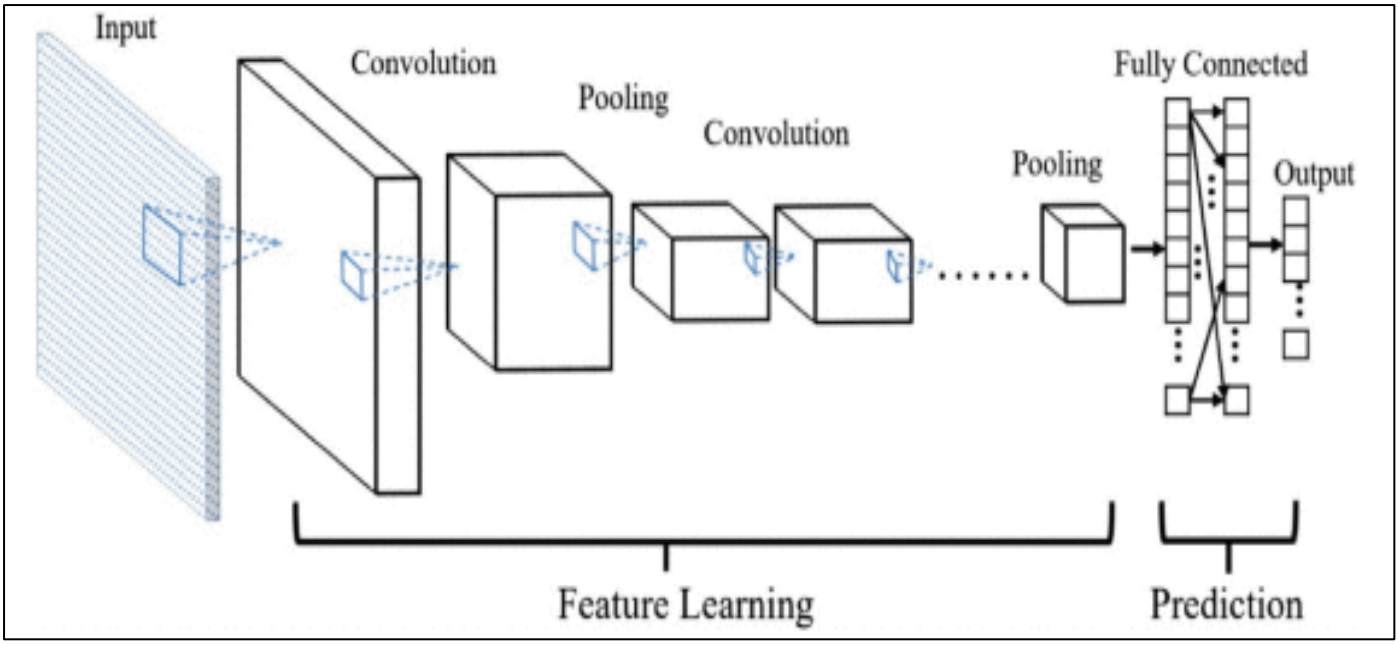

Fig 5 CNN Architecture

The Convolutional neural network, combining them, and fully linked layers comprise the CNN's hidden layers shown in Figure 5.

IV. CHALLENGES IN CREDIT CARD FRAUD DETECTION

The performances for detecting fraud in digital payment systems have advanced significantly, yet there are still numerous obstacles and unanswered questions[25][26]. These problems need more investigation because they lower the efficacy and efficiency of initiatives to prevent fraud. Here are a few of the most significant issues and open questions:

- It is essential to minimize financial damages by exposing fraudulent activities as soon as feasible. Despite significant advancements, many current fraud detection systems still face difficulties despite their real-time detection capabilities[27][28].
- To apply sophisticated analytical methods within limited periods and manage massive volumes of info from transactions in real time, technological challenges must be addressed.
- The strategies used by fraudsters to evade detection are likewise ever-evolving. It may be challenging to detect these dynamic fraud trends with traditional methods. The authors contend that more research is necessary to create

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

detection tools that can quickly recognize and respond to emerging forms of fraud[29].

- There are privacy concerns since identifying fraud occasionally necessitates examining confidential customer data. It's challenging to strike a balance between protecting consumers' personal information and effectively identifying fraud[30][31]. It will need more work to create privacy-preserving techniques for detecting forged information that are reliable with no jeopardizing the safety of data.
- The fact that fraudulent methods are always changing presents another difficulty[32]. The techniques used by scammers also evolve with detection systems, creating a never-ending game of cat and mouse.

V. LITERATURE REVIEW

The second part provides a review of the literature. A significant problem for companies that invest involves credit card theft detection, which necessitates advanced techniques to identify fraudulent transactions, as Table I summarizes.

Appavu (2025) the expanding badly-behaved of credit card fraud, emphasizing how pervasive it is becoming as e-commerce and internet payment methods gain traction. The rise in online transactions has made fraud detection a major worry, prompting academics to look at a number of ML techniques. This study offers a brand-new transaction data-based fraud detection technique. In order to identify patterns in consumer behavior, the method comprises classifying cards based on their spending, merging transactions within these categories using a window that moves technique, and looking at past transaction data. Distinct classifiers, such as LR and DT models[33].

Chaitanya et al. (2024) globally, credit card fraud is a significant problem that impacts both individuals and businesses. The Bayesian Belief Network (BBN) and Hidden Naive Bayes (HNB) techniques are used in algorithms for identifying fraudulent use of credit cards. In a dataset with several transaction characteristics, it seeks to create precise models for detecting fraudulent dealings based on these traits, HNB and BBN use probabilistic thinking and mathematical modelling to assess if a transaction is fake Performance measures are used to assess the models. The results indicate that BBN achieved 89.59% accuracy while HNB achieved 86.87%. Furthermore, HNB and BBN's competitive performance is highlighted by a comparison with alternative fraud detection techniques[34].

Sreekala et al. (2024) a major danger to financial institutions, Regarding accurate and timely being identified, credit card theft requires advanced procedures. In order to detect credit card fraud, this study combines five different categorization algorithms—RF, DT, K-NN, SVC, and NB—with the use of unsupervised learning, namely K-means clustering. The procedure uses K-means segmentation to arrange transactions based on their attributes and then uses the cluster assignments as pseudo-labels to train the classification models. The goal is to improve fraud detection's precision and effectiveness by utilizing both clustering and classification's advantages[35].

Bonkoungou et al. (2023) as the volume of cashless transactions rises, so does credit card fraud. As more individuals use mobile wallets and credit cards, the number of transactions conducted online is increasing. As internet purchasing has grown, credit card fraud has increased rapidly. Investigating the borrower's expenditures is one method of spotting credit card fraud patterns. The transaction may be considered fraudulent if there is any strange behavior. Frequent profile variations differentiating agreements that are dishonest and those that are real are only one of the numerous challenges in identification. Researchers employ a variety of methods to identify credit card fraud, including naiveté and hidden models. Bayes classifier, LR, KNN classifier, and DT[36].

Kaur et al. (2022) examines a credit card transaction's authenticity before it is processed. It is also necessary to notify the credit card owner if it turns out to be fraudulent. The technique uses extremely uneven and skewed training different ML and DL algorithms for identifying fraudulent transactions using transactional information in order to prevent missing any fraud instances with high recall or accurately predicting an excessive number of non-fraud cases. Then, we compare the models' accuracy and test results to determine which model is best[37].

Mahajan et al. (2023) one of the most common issues in today's culture is credit card theft. This kind of fraud generally happens when the perpetrator uses the credit card details of another person. One approach for spotting fraudulent behavior in one way to identify credit card fraud is via credit card transactions. use a variety of theories and methods to detect false transactions. One method that is taken into consideration is LR .The procedure that has the highest accuracy will be used to detect the fraud. The LR method's accuracy will be nearer 0.99%. They can identify the frauds with this accuracy very fast[38].

Table 1 lists the various ML techniques for identifying credit card fraud. Problems include idea drift, data imbalance, and adaptability; to address these, hybrid models, feature engineering, and adaptive techniques are needed.

Table 1 Literature Review Summary for Credit Card Fraud Detection using Machine Learning

Reference	Methodology	Key Findings	challenges	Limitations	Future Work
Appavu, (2025)	Grouping cardholders by spending, sliding window technique, classifiers (Decision Tree, Logistic Regression)	Detected behavioral patterns for fraud detection using historical data	Differentiating subtle fraud patterns	May not adapt well to rapid changes in user behavior	Improve dynamic adaptability to changing spending behaviors

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

Chaitanya et al., (2024)	Bayesian Belief Networks (BBN), probabilistic reasoning, and Hidden Naive Bayes (HNB)	HNB: 86.87% accuracy, BBN: 89.59% accuracy, competitive with other models	Data imbalance, false positives	Dependency on feature quality and independence assumptions	Integrate feature engineering to boost prediction
Sreekala et al. (2024)	K-Means clustering plus classification (RF, DT, K-NN, SVC, NB) is a hybrid.	Combining bunching and classification improves accuracy and detection efficiency	Determining optimal cluster count	Model complexity and computational cost	Explore more hybrid unsupervised + supervised models
Bonkoungou et al. (2023)	Analysing spending patterns and using many machine learning models (Naive Bayes, DT , K-NN, and LR)	Abnormal spending patterns indicate fraud	Frequent changes in user profiles	Difficulty handling concept drift	Develop adaptive models that evolve with user behavior
Kaur et al., (2022)	Comparison of ML and DL models on imbalanced datasets	Focus on high recall and high precision for better fraud detection	High false positive rate	Imbalanced data affects classifier performance	Apply advanced resampling or cost-sensitive methods
Mahajan et al. (2023)	Logistic Regression applied to transaction classification	Logistic regression achieved ~99% accuracy	Identity theft detection	Limited to linear decision boundaries	Evaluate and integrate deep learning models

VI. CONCLUSION

In addition to the business and customer, credit card theft affects the financial institution. VISA and MasterCard both utilize fraud detection algorithms. The most recent method that is being applied in many fields is the neural network because of its strong learning and prediction capabilities. ML has shown itself to be a powerful tool in the battle towards credit card fraud, providing models for prediction that lower the number of false positives and increase detection rates. However, despite advancements, several challenges remain, including real-time processing limitations, data privacy concerns, and the adaptability of fraudsters. High fraud detection accuracy has been shown by NN, DT, and LR are examples of supervised learning algorithms, while unsupervised methods like clustering and autoencoders offer more possibilities for anomaly identification.

Future studies should concentrate on hybrid models that to be a powerful tool in the battle against credit card fraud, providing predictive models that lower false positives and increase detection rates. Additionally, more work is needed to address real-time processing challenges and ensure robust security measures that balance fraud detection effectiveness with customer privacy. In the digital financial sector, federated learning techniques combined with blockchain technology may potentially provide interesting ways to reduce the risk of fraud.

REFERENCES

[1]. A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, “Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach,” Big Data Cogn. Comput., 2024, doi: 10.3390/bdcc8010006.

[2]. P. Chatterjee, “Smart Contracts and Machine Learning: Exploring Blockchain and AI in Fintech,” Indian J. Sci. Technol., vol. 18, no. 2, pp. 113–124, Jan. 2025, doi: 10.17485/IJST/v18i2.3838.

[3]. V. Pillai, “Integrating AI-Driven Techniques in Big Data Analytics: Enhancing Decision-Making in Financial Markets,” Int. J. Eng. Comput. Sci., vol. 12, no. 7, 2023.

[4]. O. Kazeem, “FRAUD DETECTION USING MACHINE LEARNING,” 2023. doi: 10.13140/RG.2.2.12616.29441.

[5]. T. Berhane, T. Melese, A. Walelign, and A. Mohammed, “A Hybrid Convolutional Neural Network and Support Vector Machine-Based Credit Card Fraud Detection Model,” Math. Probl. Eng., 2023, doi: 10.1155/2023/8134627.

[6]. 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, 2022, doi: 10.1109/ACCESS.2022.3166891.

[7]. R. Bin Sulaiman, V. Schetinin, and P. Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection,” Human-Centric Intell. Syst., 2022, doi: 10.1007/s44230-022-00004-0.

[8]. Y. Jain, N. Tiwari, S. Dubey, and S. Jain, “A comparative analysis of various credit card fraud detection techniques,” Int. J. Recent Technol. Eng., 2019.

[9]. N. Yousefi, M. Alaghband, and I. Garibay, “A Comprehensive Survey on Machine Learning Techniques and User Authentication Approaches for Credit Card Fraud Detection,” pp. 1–27, 2019, [Online]. Available: http://arxiv.org/abs/1912.02629

[10]. J. K. Afriyie et al., “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” Decis. Anal. J., vol. 6, no. November 2022, pp. 1–12, 2023, doi: 10.1016/j.dajour.2023.100163.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

[11]. V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," Lib. Media Priv. Ltd., 2022.
[12]. V. Pillai, "Enhancing Transparency and Understanding in AI Decision-Making Processes," irejournals, vol. 8, no. 1, p. 5, 2024.
[13]. M. I. Khan, A. Arif, and A. R. A. Khan, "AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity," BIN Bull. Informatics, vol. 2, no. 2, pp. 248–261, 2024.
[14]. S. Bonkoungou, N. R. Roy, N. H. A. E. J. Ako, and A. Mishra, "Credit Card Fraud Detection Using ML Techniques," Lect. Notes Networks Syst., vol. 896, no. 2, pp. 15–23, 2024, doi: 10.1007/978-981-99-9811-1_2.
[15]. A. Gogineni, "Advancing Kubernetes Network Stack for High-Performance AI/ML Workloads," Int. J. Sci. Technol., vol. 15, no. 4, 2024.
[16]. I. Mekterović, M. Karan, D. Pintar, and L. Brkić, "Credit Card Fraud Detection in Card-Not-Present Transactions: Where to Invest?," Appl. Sci., vol. 11, no. 15, 2021, doi: 10.3390/app11156766.
[17]. S. Tyagi, T. Jindal, S. H. Krishna, S. M. Hassen, S. K. Shukla, and C. Kaur, "Comparative Analysis of Artificial Intelligence and its Powered Technologies Applications in the Finance Sector," in Proceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022, 2022. doi: 10.1109/IC3I56241.2022.10073077.
[18]. T. K. Dang, T. C. Tran, L. M. Tuan, and M. V. Tiep, "Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems," Appl. Sci., 2021, doi: 10.3390/app112110004.
[19]. V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, "Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning," Information, vol. 15, no. 8, p. 478, Aug. 2024, doi: 10.3390/info15080478.
[20]. A. V. Hazarika and M. Sha, "Exploring Fault Tolerance Strategies In Big Data Infrastructures And Their Impact On Processing Efficiency," SSRN Electron. J., 2025, doi: DOI:10.2139/ssrn.5078913.
[21]. S. Tyagi, "Analyzing Machine Learning Models for Credit Scoring with Explainable AI and Optimizing Investment Decisions," vol. 5, no. 01, pp. 5–19, 2022, [Online]. Available: http://arxiv.org/abs/2209.09362
[22]. M. A. Rassam, "Autoencoder-Based Neural Network Model for Anomaly Detection in Wireless Body Area Networks," IoT, vol. 5, no. 4, pp. 852–870, 2024, doi: 10.3390/iot5040039.
[23]. E. A. L. M. Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," PeerJ Comput. Sci., vol. 9, pp. 1–66, 2023, doi: 10.7717/PEERJ-CS.1278.
[24]. I. D. Mienye and N. Jere, "Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions," IEEE Access, vol. 12, no. July, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.
[25]. S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure : Ensuring Compliance and Security in Utility Systems," vol. 8, no. 2, pp. 1–8, 2022.
[26]. S. S. S. Neeli, "Securing and Managing Cloud Databases for Business - Critical Applications," J. Eng. Appl. Sci. Technol., vol. 7, no. 1, p. 6, 2025.
[27]. V. Pillai, "Anomaly Detection Device for Financial and Insurance Data," p. 2025, 2025.
[28]. S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. Paul Aderemi, "Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches," 4th Int. Conf. Innov. Pract. Technol. Manag. 2024, ICIPTM 2024, p. 364, 2024, doi: 10.1109/ICIPTM59628.2024.10563348.
[29]. M. S. Samarth Shah, "Deep Reinforcement Learning For Scalable Task Scheduling In Serverless Computing," Int. Res. J. Mod. Eng. Technol. Sci., vol. 3, no. 12, pp. 1845–1852, 2021, doi: DOI : https://www.doi.org/10.56726/IRJMETS17782.
[30]. S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," 2021, doi: https://doi.org/10.36948/ijfmr.2021.v03i04.34396.
[31]. S. R. Thota, S. Arora, and S. Gupta, "Hybrid Machine Learning Models for Predictive Maintenance in Cloud-Based Infrastructure for SaaS Applications," 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691295.
[32]. K. Patel, "Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques," Int. J. Comput. Trends Technol., 2023, doi: 10.14445/22312803/ijctt-v71i10p109.
[33]. N. Appavu, "AI and ML Approaches for Credit Card Fraud Detection: A Comparative Study of Logistic Regression and Decision Tree Techniques," in 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 2025, pp. 2068–2074. doi: 10.1109/IDCIOT64235.2025.10915092.
[34]. G. S. Chaitanya, K. Deepika, G. S. Prabhav, R. B. Patil, and M. A. Jabbar, "Credit Card Fraud Detection using Hidden Naive Bayes and Bayesian Belief Network," in 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), 2024, pp. 1–6. doi: 10.1109/I2CT61223.2024.10544328.
[35]. K. Sreekala, R. Sridivya, N. K. K. Rao, R. K. Mandal, G. J. Moses, and A. Lakshmanarao, "A hybrid Kmeans and ML Classification Approach for Credit Card Fraud Detection," in 2024 3rd International Conference for Innovation in Technology (INOCON), 2024, pp. 1–5. doi: 10.1109/INOCON60754.2024.10511603.
[36]. S. Bonkoungou, N. R. Roy, N. H. A.-E. Ako, and U. Batra, "Credit Card Fraud Detection using ML: A Survey," in 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), 2023, pp. 732–738. doi: 10.1109/IITCEE57236.2023.10091035.
[37]. D. Kaur, A. Saini, and D. Gupta, "Credit Card Fraud Detection Using Machine Learning, Deep Learning, and Ensemble of the both," in PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1813

Grid Computing, 2022. doi: 10.1109/PDGC56933.2022.10053175.

[38]. A. Mahajan, V. S. Baghel, and R. Jayaraman, "Credit Card Fraud Detection using Logistic Regression with Imbalanced Dataset," in Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023, 2023.