Deep Learning-based Anomaly Detection in Credit Card Transactions

Farhat Lamia Barsha
Department of Computer Science, Tennessee Technological University
fbarsha42@tntech.edu

***Abstract*— The issue of credit card fraud continues to be a prevalent concern in the modern era of digital technology, leading financial institutions to implement advanced fraud detection systems. Although these solutions have undeniably improved security measures, the ongoing issue of false positives remains a prevalent concern within the sector. False positives refer to instances where valid transactions are mistakenly identified as fraudulent, resulting in negative consequences such as customer discomfort, diminished trust, and increased operational expenses. This study provides a critical analysis of false positives in credit card fraud detection, presenting a thorough examination of its underlying causes and potential consequences. I have applied Convolutional neural network (CNN) and Artificial neural network (ANN) to identify credit card fraud and analyze the false positive occurrence. In order to mitigate the occurrence of false positive cases, this study suggests addressing the imbalance within the dataset. The findings indicate that both CNN and ANN exhibit superior performance when applied to a balanced dataset. Additionally, it is vital to emphasize that precision, recall, and F1 score are more significant performance evaluation metrics than accuracy when assessing credit card fraud detection systems. The study also suggests optimizing CNN and ANN models for credit card fraud detection. Tuning hyperparameters, optimizing feature selection, and researching ensemble approaches to balance false positives and fraud detection are all part of this.**

***Keywords*—Credit card fraud, Anomaly detection, Financial transactions, Cyber Security, Fraud Detection, Deep learning.**

I. INTRODUCTION

Credit card fraud is an expression of identity theft that happens when an individual obtains someone's private information without authorization and uses it for financial transactions. The utilization of credit cards has recently experienced a significant rise due to the rapid growth of online transactions. As credit card utilization continues to increase, so does the risk of fraudulent activity, which can result in substantial financial losses for individuals and institutions [1].

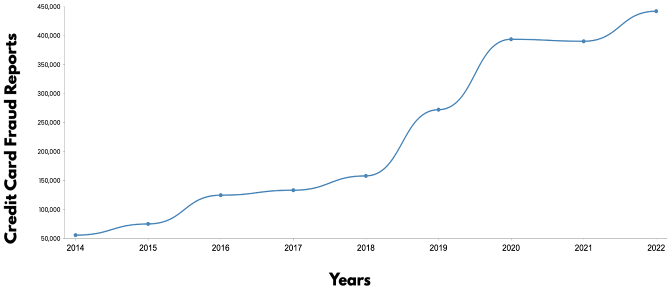

Fig. 1: Credit card fraud in the United States by year [2]

According to the Nilson Report's December 2022, it is projected that global losses resulting from card fraud will amount to $397.4 billion within the upcoming decade. Notably, the United States is anticipated to account for $165.1 billion of these losses [3]. The United States experienced a 13% rise in credit card fraud cases from 2021 to 2022 as shown in Figure 1.

Criminals execute fraudulent activities by either physically stealing credit cards or obtaining card information for online use. There are two types of credit card fraud: (1) Card present fraud and (2) Card-not-present fraud. Figure 2 represents different forms of credit card fraud.

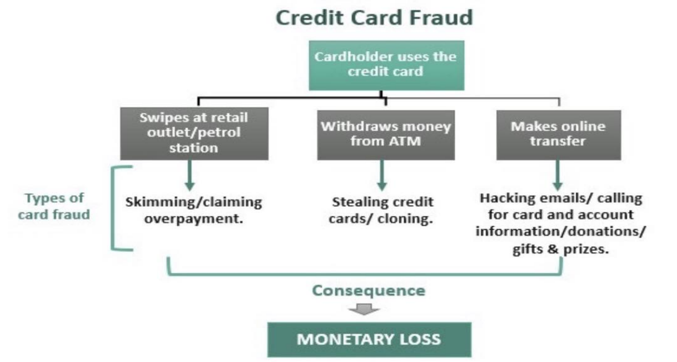
Credit Card Fraud
Cardholder uses the credit card
Swipes at retail outlet/petrol station
Withdraws money from ATM
Makes online transfer
Types of card fraud
Skimming/claiming overpayment.
Stealing credit cards/ cloning.
Hacking emails/ calling for card and account information/donations/ gifts & prizes.
Consequence
MONETARY LOSS

Fig. 2: Credit card Fraud categories

Card present fraud refers to the illegal use of a physical card which can be obtained through theft, such as robbery, pick-pocketing, mail theft, or replication [4]. To make a duplicate card, criminals may exploit card skimmers that are installed at commonly utilized payment terminals to gather and retain card information during the swiping process. A skimming attack takes place when attackers attach a device onto a credit card reader with the purpose of secretly acquiring the magnetic stripe data of the card during the act of swiping. Card skimming refers to a form of cybercrime that involves the unauthorized acquisition of sensitive payment data by means of deploying malicious software, commonly referred to as a card skimmer, on an e-commerce platform.

Card-not-present fraud is a type of fraudulent activity in which the fraudster utilizes card-related information, including the card number, account holder name, and CVV code, without physically possessing the card [5]. (1) The electronic communications, such as emails or text messages, may potentially include a hyperlink directing users to a fraudulent website designed to resemble the authentic website. When a user submits their credit card information on the fraudulent website, the attackers illegally access the data. (2) Malware targeting credit card transactions refers to a form of malicious software designed with the intent to illicitly acquire credit card data [6]. The installation of malware on computers or mobile devices can occur silently and without the explicit approval or awareness of the user. Subsequently, this malware can be utilized to illicitly gather credit card information from websites, online businesses, and various other online transactions. (3) A data breach involving credit card transactions refers to the illegal acquisition of sensitive credit card information, including card numbers, expiration dates, and CVV codes [7]. (4) Phishing attacks are a form of cybercriminal activity wherein attackers send fraudulent emails or text messages that replicate the appearance of authentic communications originating from trustworthy entities, such as financial institutions or credit card companies [6]. Figure 3 represents 8 commonly occurring cyber threats.

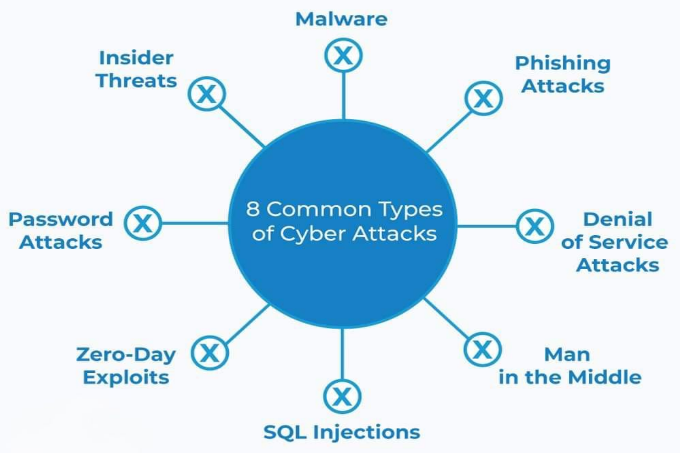

Fig. 3: Types of cyber security threats

Since 2015, there has been a significant shift in credit card fraud, with a notable increase in card-not-present criminal activities. The primary factor contributing to this phenomenon can be attributed to the implementation of EMV (Europay, MasterCard, and Visa) chip technology by prominent credit card corporations on a global scale [8].

Credit card fraud detection includes various methods financial institutions employ to mitigate, detect, and effectively handle incidents of credit card fraud. Digital and automated methods are commonly employed for the detection of credit card fraud. Certain financial institutions employ artificial intelligence (AI) and machine learning techniques to examine customer behavior, including their patterns of expenditure and credit utilization, with the purpose of identifying any unexpected account activity [9]. The credit card fraud detection process includes parameterization, training, and detection [10]. Figure 2 represents the integration of data collection, data preprocessing, and modeling within the parameterization phase. The training phase encompasses both the modeling process and the application of fraud detection techniques. The detection phase consists of the evaluation of results and the assessment of model performance.

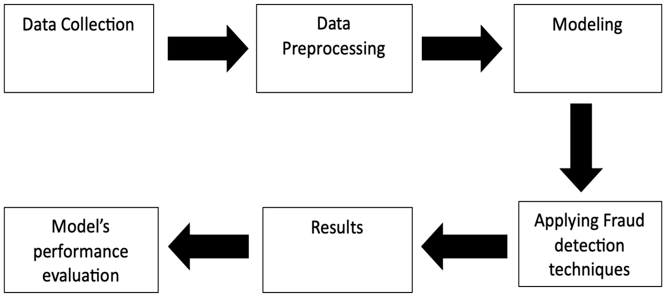
Data Collection
Data Preprocessing
Modeling
Applying Fraud detection techniques
Results
Model's performance evaluation

Fig. 4: Credit card fraud detection process

Machine learning classification algorithms involve supervised learning, unsupervised Learning, semi-supervised learning, or reinforcement Learning [11][12]–[19]. Supervised learning is a machine learning approach that uses a training set to instruct models on how to produce the desired output. Logistic Regression, Naive Bayes, Random Forest, Support Vector Machine, Neural Networks [20][21][22], etc., are examples of supervised learning [23][24][25]. Unsupervised learning is a machine learning technique which evaluate and cluster datasets without explicit labels. K-Means Clustering, Principal Component Analysis, Hierarchical Clustering, etc., are examples of unsupervised learning [26] [24]. Semi-supervised learning aims to assign labels to unlabeled data instances by using the knowledge acquired from a limited set of labeled data instances [1]. Image classification, facial recognition, etc., are examples of semi-supervised learning. Reinforcement learning involves training a computational model to iteratively make decisions in order to get an optimal solution for a given problem [27]. This process is characterized by the model's ability to learn from its own experiences and adjust its decision-making strategy accordingly. Q-learning, K nearest neighbors algorithm, DQN, etc., are examples of reinforcement learning.

Fraud detection systems are always evolving, becoming increasingly robust and efficient over time. However, it is important to note that these strategies are not without limitations. Various challenges in credit card fraud detection still exist, including imbalanced datasets, overlapping data, misclassification, constrained datasets, changing fraud patterns over time, feature generation, fraud detection cost, lack of standard metrics, etc. [28][29][16]. Figure 5 displays a tree diagram illustrating different aspects of credit cards and the methodologies employed to identify anomalies and mitigate cyber-attacks. The false positive rate is a significant challenge in the realm of credit card fraud detection. The occurrence of

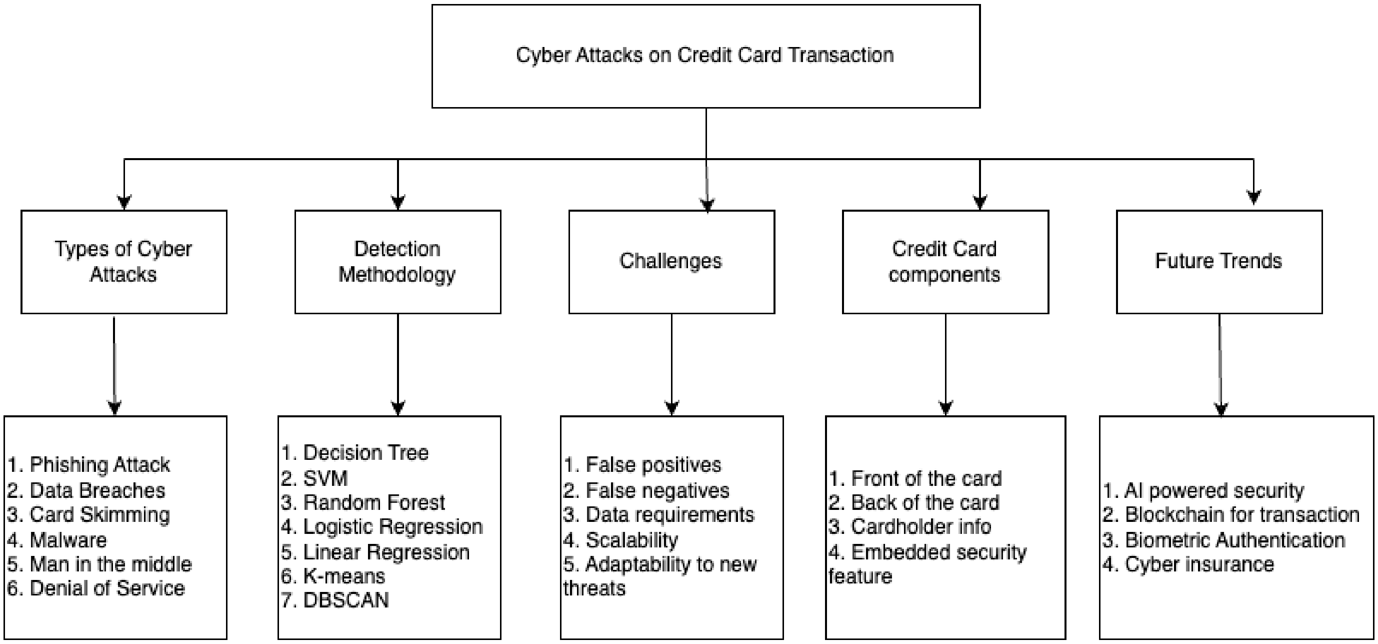

Fig. 5: Tree Diagram of the different aspects of Anomaly Detection on Credit Card Transaction

erroneously classifying a legitimate transaction as a fraudulent one, referred to as a false positive, has significant financial and reputational implications.

False positives must be carefully considered while designing strong and dependable systems. Users whose legitimate transactions cause false warnings may lose trust in the system and financial institution. This deterioration might strain customer relations because consumers may view the fraud detection system as unreliable or too cautious. Financial institutions also suffer economically from false positives. Manual reviews, customer support interventions, and potential compensation measures add to operational overhead when researching and resolving these issues. Beyond financial concerns, false positives cost customers and merchants missing chances and refused transactions. The fiscal consequences and potential business loss highlight the need of credit card fraud detection precision.

The incorporation of deep learning techniques, specifically Convolutional Neural Networks (CNNs) and Artificial Neural Networks (ANNs), has had a significant influence on the field of credit card fraud detection. This impact is mostly attributed to the notable decrease in instances of false positive outcomes. These algorithms demonstrate exceptional performance in the identification of complex patterns and the acquisition of features, effectively adjusting to changing fraud patterns without significant dependence on manual rule-based systems. The capacity to effectively manage imbalanced datasets, perform hierarchical feature extraction, and employ ensemble learning techniques significantly enhances the accuracy and precision of identifying fraudulent transactions, hence mitigating the occurrence of false positives.

The key contributions of this work are as follows:

1) **Deep Learning methods on anomaly detection:**Deep learning exhibits superior performance compared to conventional machine learning algorithms in the domain of credit card fraud detection, owing to its inherent ability to autonomously extract complicated characteristics from data, comprehend sophisticated patterns, and adjust to dynamic fraud techniques.
2) **Algorithmic Equivalence:** Both CNN and ANN show comparable performance in credit card fraud detection within a balanced dataset.
3) **False Positive and False Negative Rates:** The CNN algorithm exhibits remarkable efficacy in mitigating occurrences of false positives. In contrast, the ANN algorithm has exceptional efficacy in reducing the occurrence of false negatives.
4) **Emphasis on Precision, Recall, and F1 Score:** The study underscores the significance of precision, recall, and F1 score over accuracy for evaluating credit card fraud detection systems.

The subsequent sections of the paper are structured as follows: In section II, a thorough analysis of the related existing work done by current scholars was presented. In Section III, the paper presents the problem definition, system model and outlines the proposed solution methodology. In Section IV, the result and discussion of the obtained results are presented. The paper is concluded in section V with future research directions.

II. Research Overview

This section examines relevant current research in the literature on various methodologies for anomaly detection. This paper focuses on the specific aspects of anomaly detection in credit card transactions. Figure 5 displays a tree diagram illustrating the many components of credit card fraud and the methodologies employed to identify and address anomalies. The tree diagram includes the classification of anomalies, several criteria for anomaly identification, the layers and components of a credit card, and the significant computational algorithms or approaches associated with them. There are five sub-sections that have been established within the domain of anomaly detection in credit card transactions. These subsections are categorized as follows: types of cyber attacks, methodology for anomaly detection, obstacles encountered in this field, components of credit cards, and future developments in this domain.

The motivation behind employing deep learning methods for anomaly detection in credit card fraud stems from the inherent complexity and dynamic nature of fraudulent activities. Conventional approaches frequently encounter difficulties in accurately detecting the complex patterns and small irregularities that are indicative of fraudulent activities in credit card transactions. The utilization of deep learning, which possesses the capacity to autonomously acquire hierarchical representations and discover intricate relationships between datasets, offers a highly convincing resolution. The motivation behind this endeavor is rooted in the need to develop a fraud detection system that is both adaptive and accurate, capable of independently evolving to effectively recognize newly developing patterns of fraudulent activity. The increasing sophistication of fraudsters necessitates the utilization of deep learning models, which provide crucial robustness and adaptability. Moreover, the extensive and disproportionate characteristics of credit card transaction datasets require an approach that can proficiently address these complexities, rendering deep learning an attractive option due to its ability to acquire knowledge from extensive and varied datasets. The rationale behind the use of deep learning in credit card anomaly detection stems from its capacity to offer a more advanced, adaptive, and precise safeguard against the ever-evolving realm of fraudulent behaviors.

The selected papers and the strategies or procedures employed are presented in Table I. The following paragraphs includes a concise overview of the selected papers.

In P1, the authors have conducted an investigation on the identification and prevention of fraud in digital transactions using advanced machine learning and deep learning techniques. In P2, the authors provide a comprehensive overview of recent advancements in statistical and machine-learning techniques for the detection of financial fraud. These techniques include graph neural networks, node2vec, and dynamic weighted entropy, among others. The review provides a concise overview and introduces the fundamental concept of these novel methodologies.

In P3, The researchers employed four machine learning techniques, namely decision tree, random forest, logistic regression, and Naïve Bayes, to train the models. Furthermore, the utilization of deep neural networks in model training has demonstrated more favorable outcomes in contrast to conventional machine learning algorithms. A comparative analysis has been conducted to assess the accuracy of each algorithm employed in the implementation of credit card fraud detection. The objective of P4 is to employ various machine learning algorithms, including Logistic Regression, K-Nearest Neighbor, and Random Forest, as well as deep learning techniques such as Deep Neural Network and Convolutional Neural Network, in the analysis of a real-world credit card dataset. The purpose is to determine the most effective approach for identifying fraudulent transactions. After conducting many trials with varied settings utilizing all the aforementioned algorithms, it was shown that the Random Forest Algorithm exhibits marginally superior accuracy compared to Deep Neural Networks.

In P5, the authors conduct an investigation and provide a comprehensive analysis of the popular and efficient anomaly detection methods utilized emphasizing the latest breakthroughs in the domains of semi-supervised and unsupervised learning techniques for the identification of financial fraud. In P6, the authors present a deep learning-based credit card fraud detection system. An artificial neural network (ANN) with 100% accuracy is optimal for credit card fraud detection in their model comparing it to the k-nearest Neighbor, Support vector machine, etc.

In P7, it is stated that a range of approaches can be employed for the identification of credit card fraud. The artificial neural network (ANN) technology is well-suited for the identification of fraudulent transactions. Simulated annealing is a computationally intensive procedure. The genetic algorithm is capable of identifying the most optimal solution from a given set of options based on its effectiveness. In P8, the authors first analyze a typical credit card recognition problem, including the dataset, attributes, metric selection, and strategies for handling unbalanced datasets, and then discuss methods for capturing credit card transaction sequences. In P9, the authors present a thorough examination of diverse fraud detection approaches included in the detection models offered by numerous researchers. It also discusses the datasets utilized in their research and the various evaluation factors employed to assess the effectiveness of their models.

TABLE I: List of the selected research papers on anomaly detection in credit card transactions

SI	Paper	Techniques/Tools used	Anomaly detection challenges discussed	Detection techniques limitations discussed
P1	[22]	Machine Learning + Deep Learning	✓	
P2	[30]	Deep Learning	✓	
P3	[31]	Machine Learning + Deep Learning		
P4	[32]	Machine Learning + Deep Learning		
P5	[11]	Machine Learning + Deep Learning		
P6	[33]	Machine Learning + Deep Learning		
P7	[34]	Machine Learning + Deep Learning + Hybrid approach	✓	
P8	[35]	Machine Learning		
P9	[28]	Machine Learning + Deep learning + Hybrid approach		✓
P10	[36]	Sampling Techniques		
P11	[37]	Machine Learning + Sampling Techniques		✓
P12	[38]	Machine Learning + Deep Learning	✓	
P13	[39]	Deep Learning		
P14	[40]	Deep Learning		
P15	[20]	Deep Learning		

In P10, the authors has conducted an examination of various sampling technique approaches that are capable of effectively addressing the issue of imbalanced data inside the credit card transaction dataset. The proposed optimal solution involves using a hybrid approach that combines the most effective sampling strategies. This approach aims to achieve a balanced dataset and enhance the performance of the detection system. In P11, the authors demonstrate a current lack of comprehensive exploration into deep learning, indicating the need for further investigation to tackle the difficulties involved with identifying credit card fraud using emerging technologies like big data analytics, large-scale machine learning, and cloud computing.

P12 examines various machine learning algorithms employed in the detection of credit card fraud like decision tree, logistic regression, random forest etc, while also considering the advantages and disadvantages associated with these methodologies. P13 examines deep learning strategies for credit card fraud detection and compares them to machine learning algorithms on three financial datasets. Experimental results reveal that deep learning methods outperform classical machine learning models, suggesting they can be used in real-world credit card fraud detection systems.

The purpose of the research P14 is to create a powerful deep learning model for detecting credit card fraud. We discovered that logistic and hyperbolic tangent activation functions effectively detect credit card fraud. The logistic activation function is more effective with 10 nodes (82% sensitivity) and 100 nodes (83% sensitivity) in the 3 hidden layer model. The hyperbolic tangent activation function is more effective with 1000 nodes, with 82% sensitivity for hidden layers (1, 2, and 3). In P15, three advanced data mining approaches, NN, MPL, and CNN, were evaluated for credit card fraud detection using a unique credit card transaction dataset for examination. Among these approaches, the multilayer Perceptron excelled in credit card fraud detection on their unique and general dataset.

This study examines the implications of false positive cases in credit card fraud detection and proposes the implementation of sampling techniques as a means to mitigate this issue. Additionally, the discussion revolved around the importance of considering precision and recall as assessment metrics for assessing the efficacy of anomaly detection techniques, as opposed to relying just on accuracy.

Based on the previously mentioned literature reviews, it is important to note that the following technological constraints have been identified:

1) There is currently a lack of research that specifically examines the consequences of false positive cases and strategies to mitigate their occurrence.
2) Most research has been focused on accuracy metric to measure the effectiveness of anomaly detection techniques.
3) In order to address the aforementioned concerns, this study introduces a sampling technique aimed at mitigating the occurrence of false positive cases. Furthermore, the significance of precision and recall in evaluating the efficacy of anomaly detection algorithms has been highlighted.

III. Research Problem

The primary issue addressed in this research study pertains to the identification and detection of anomalies inside credit card transactions. The system has been designed to identify anomalies while also minimizing the occurrence of false positive cases in order to improve precision and recall. This section will include an analysis of the system model, a formal explanation of the problem, and a proposed solution methodology.

A. *Formal definition of the problem:*

The formal definition of anomaly detection in credit card transactions entails the systematic identification of deviations from anticipated or standard patterns within a given dataset of credit card transactions. Formally, let D represent the set of all credit card transactions, F denote the subset of transactions labeled as anomalies or potentially fraudulent, and N represent the subset of transactions labeled as non-anomalous or legitimate. Anomaly detection involves the identification of instances x in subset D such that $x \in F$ is based on features and patterns that deviate significantly from the established norm.

The issue of false positive occurrences in the realm of credit card fraud detection pertains to situations in which a valid financial transaction is erroneously identified as fraudulent by the detection mechanism. Formally, let D represent the set of all credit card transactions, F denote the subset of transactions labeled as fraudulent, and N represent the subset of transactions labeled as non-fraudulent. False positives occur when a transaction x in subset N is misclassified as fraudulent, i.e., $x \in N$ but is assigned the label F. The primary goal of credit card fraud detection is to optimize the balance between minimizing false positives and maximizing the accurate identification of truly fraudulent transactions.

B. *System model:*

The Anomaly detection process in credit card transactions is represented in figure 4. The process begins with data collection, wherein transaction details are acquired from a variety of sources. The subsequent data preprocessing module aims to enhance the raw transaction data by addressing issues such as missing values and normalization. The modeling phase encompasses the construction of a robust fraud detection model, frequently utilizing machine learning or deep learning methodologies to identify trends within the preprocessed data. The process of implementing fraud detection methods includes utilizing a trained model to evaluate novel transactions, producing anomaly scores, and categorizing them according to predetermined thresholds. The results section offers a comprehensive display of identified transactions that have been flagged, encompassing crucial details such as the transaction ID, timestamp, and anomaly scores. The module for evaluating the performance of the fraud detection model ultimately measures its efficacy by conducting a comparative analysis between its predictions and the actual outcomes. This assessment is carried out using metrics such as accuracy, precision, recall and f1-score. This modular process ensures a systematic and iterative approach to enhancing the model's ability to identify anomalies and minimize false positives and negatives in credit card transactions.

The process of achieving balance within the dataset holds significant importance in the realm of credit card fraud detection. In order to mitigate biases towards the majority class, it is imperative to utilize a balanced dataset during the training of a machine learning model. This entails ensuring that both legitimate and fraudulent transactions are equally represented, hence providing the model with equitable exposure to both classes.

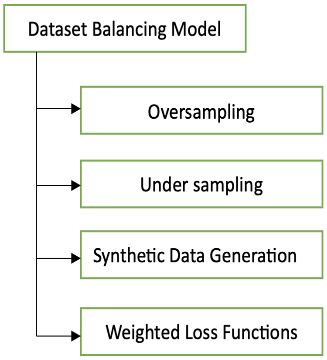

Fig. 6: Dataing Balancing Model

Oversampling involves augmenting the quantity of occurrences in the minority class, namely fraudulent transactions, in order to achieve equality with the majority class. Undersampling involves reducing the quantity of instances belonging to the majority class (regular transactions) in order to align it with the minority class. Synthetic Data Generation employs techniques such as SMOTE (Synthetic Minority Over-sampling Technique) to generate synthetic examples of the minority class, thereby augmenting the dataset. Weighted loss functions are employed to modify the loss function throughout the training process, with the aim of assigning greater significance to misclassifications in the minority class.

C. *Solution Methodology*

In order to address the problem of erroneous positive instances in the detection of credit card fraud and improve the overall efficacy of the detection system, a proposed solution model is presented that utilizes dataset balancing techniques. The proposed model consists of a set of sequential procedures. These procedures include data preprocessing, undersampling to achieve dataset stability, feature separation, data splitting, standardization, reshaping, and the utilization of CNN and ANN models. The subsequent analysis entails the assessment of the model's performance by utilizing metrics from the confusion matrix, including accuracy, precision, recall, and F1 score. The following is a comprehensive discussion of each individual step:

1) **Dataset Preprocessing:** In order to facilitate the study of the raw credit card transaction data, it is imperative to address any missing information, handle outliers, and perform any necessary cleaning processes.
2) **Undersampling for Dataset Balancing:** One approach to address class imbalance is to employ a technique that involves decreasing the number of instances in the majority class, which in this case refers to non-fraudulent transactions. This method aims to establish a more equitable representation of both classes.
3) **Feature Separation:** The dataset should be partitioned into two distinct categories: the independent variables, also known as features, and the target variable, which

represents the label indicating whether a certain instance is classified as fraud or non-fraud. In this particular scenario, the target variable represents the class, which is a numerical entity. A value of 0 signifies a real transaction, whereas a value of 1 indicates a fraudulent transaction.

4) **Dataset Splitting:** The dataset should be divided into separate training and testing sets in order to assist the training and evaluation of the model. Here I divide the dataset into 80% training data and 20% testing data.
5) **Standardization:** In order to promote the convergence of neural network models, it is imperative to standardize the feature values, hence ensuring consistency.
6) **Reshape Data:** The input data is transformed in order to conform to the network's input specifications, which often involve the use of a three-dimensional array that represents transactions.
7) **Application of CNN and ANN:** The study employed Convolutional Neural Network (CNN) and Artificial Neural Network (ANN) models to detect instances of credit card fraud. The models were trained and validated using a preprocessed dataset that had been balanced to ensure equal representation of fraudulent and non-fraudulent transactions.
8) **Evaluation Metrics Emphasis:** Emphazied to focus on precision, recall, and the F1 score rather than solely relying on accuracy. These metrics provide a more nuanced understanding of the model's performance, particularly its ability to minimize false positive cases, especially in case of anomaly detection.
9) **Analysis:** The confusion matrix and performance indicators are examined to evaluate the efficacy of the model in mitigating false positives, which refer to the misclassification of normal transactions as fraudulent, and false negatives, which pertain to the model's failure to identify genuine fraudulent transactions.

IV. Result and Discussion

In this study, we evaluate the Kaggle credit card fraud dataset with Convolutional Neural Network (CNN) and Artificial Neural Network (ANN). In the case of credit card fraud, true positive means positive cases are correctly assigned to the positive class which means that fraud transactions are correctly classified as fraud. True negative means negative cases are correctly assigned to the negative class, which means that non-fraud transactions are correctly classified as non-fraud or real transactions. The dataset is divided into train and test datasets where the training dataset consists of 80% data and the testing dataset holds 20% of the entire dataset.

In the case of CNN, at first, I got 12 false positives out of 56962 test data. The obtained results include 99% accuracy, 85% precision, 71% recall, and 78% f1-score. The dataset exhibits a significant imbalance, with just 492 instances of fraud out of a total of 284,807 data points, accounting for only 0.17% of the entire dataset. In order to enhance the performance of fraud detection, I have employed dataset-balancing techniques named undersampling. In order to achieve this, I created a non-fraud data frame with dimensions matching those of the fraud data frame, hence ensuring the compatibility of entries. Subsequently, I merged the non-fraud and fraud transaction datasets. Next, the data was scaled using the Standard Scaler method. After balancing the dataset, I got just 1 false positives out of 56962 test data. I got 91% accuracy, 98% precision, 84% recall and 90% f1-score.

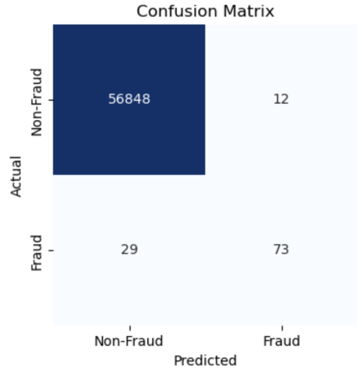

Fig. 7: Confusion Matrix by CNN in imbalanced dataset

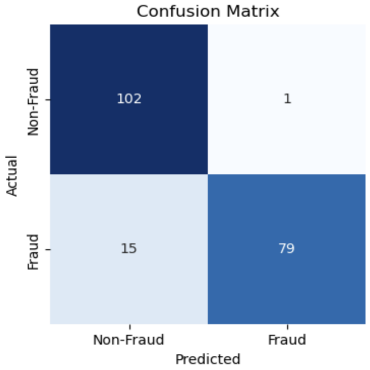

Fig. 8: Confusion Matrix by CNN in balanced dataset

Due to dataset imbalance, precision, recall, and F1 score are more important than accuracy in credit card fraud detection. With most credit card transactions being valid, a model that predicts all transactions as non-fraudulent could be accurate without detecting fraud. Metrics that focus on the positive class are needed to accurately identify infrequent fraud cases, the main goal of fraud detection.

Precision is important because it assesses the model's positive predictions' accuracy, specifically the ratio of true positives to the total projected positives, which quantifies the percentage of identified frauds that are real. Recall measures the model's capacity to identify all actual fraud cases by comparing true positives to total positives and calculating the percentage of discovered frauds among all fraudulent transactions. False positives and negatives are balanced by the harmonic mean of precision and recall, the F1 score. In situations with significant class imbalance, these metrics provide a more complete picture of a model's credit card fraud detection performance than accuracy alone. After balancing the dataset, it is observed that the accuracy metric has decreased, while there has been an improvement in the precision, recall, and f1-score metrics.

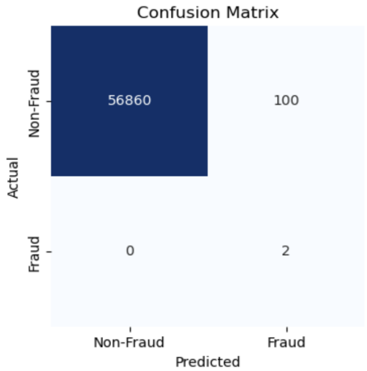

Fig. 9: Confusion Matrix by ANN in imbalanced dataset

Additionally, the dataset was subjected to the use of an Artificial Neural Network (ANN), which is another deep learning method. In the imbalanced dataset, there were initially 100 instances classified as false positives. However, after balancing the dataset, this number decreased to 16. In the case of an imbalanced dataset, an accuracy rate of 99%, precision of 100%, recall of 2% and f1-score of 4% was achieved. For a balanced dataset, the obtained results include an accuracy of 91%, precision of 98%, recall of 82%, and a f1-score of 90%.

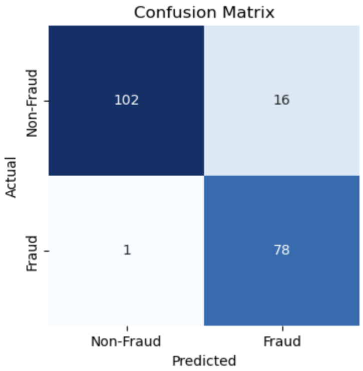

Fig. 10: Confusion Matrix by ANN in balanced dataset

When comparing the performance of the CNN and ANN algorithms in a balanced dataset, it is seen that both algorithms exhibit similar performance in the context of credit card fraud detection. However, the CNN algorithm demonstrates a lower rate of false positive cases, while the ANN algorithm exhibits a lower rate of false negative cases.

From Table II we can see the following findings-

TABLE II: Comparsion between CNN and ANN

	CNN (Imbalanced)	CNN (Balanced)	ANN (Imbalanced)	ANN (Balanced)
Accuracy	99	91	99	91
Precision	85	98	100	98
Recall	71	84	2	82
F1-score	78	90	4	90

1) The CNN model demonstrates superior performance compared to the ANN model in terms of precision, recall, and F1 score, regardless of whether the datasets are imbalanced or balanced. This implies that the CNN design demonstrates greater efficacy in collecting intricate patterns and features linked to credit card fraud.
2) The utilization of balanced datasets yields enhanced recall rates, indicating that the models exhibit improved capacity to accurately identify a greater number of instances of genuine fraudulent activity. The precision of the results remained at a high level, indicating a low occurrence of false positives.
3) The only reliance on accuracy as a statistic for credit card fraud detection may not provide comprehensive information, particularly when dealing with imbalanced datasets. Precision, recall, and F1 score offer a more comprehensive evaluation of the model's performance, highlighting the significance of effectively managing the balance between false positives and false negatives.

Overall, the analysis emphasizes dataset balancing and CNN architectures' credit card fraud detection. It also stresses that fraud detection models should be evaluated on precision, recall, and F1 score over accuracy.

V. Conclusion

This study has revealed significant findings about the performance of Convolutional Neural Networks (CNN) and Artificial Neural Networks (ANN) in the context of credit card fraud detection using a balanced dataset. The similarity in performance between the two algorithms highlights their comparative effectiveness in achieving the overall objective of fraud detection. Upon further analysis, it becomes evident that there are notable strengths associated with both the CNN algorithm and the ANN algorithm. The CNN algorithm demonstrates exceptional proficiency in reducing instances of false positives, which confers a significant benefit in safeguarding the authenticity of legitimate transactions. On the other hand, the ANN algorithm exhibits superior performance in minimizing false negatives, thereby enhancing the effectiveness of security measures. Along with this, by acknowledging the importance of precision in minimizing the impact of false positives and recognizing the crucial function of recall in detecting fraudulent actions, the framework of performance assessment in credit card fraud detection is redefined.

Future studies could explore the potential benefits of incorporating explainability and interpretability properties into neural network models. Gaining insight into the decision-making mechanisms employed by these models helps build trust among end-users and regulatory entities, hence promoting the integration of advanced algorithms inside the financial industry.

Furthermore, there is potential for future exploration of the integration of temporal and sequential elements in credit card transaction data. The utilization of time-series analysis with recurrent neural networks has the potential to provide valuable insights into the dynamic characteristics of fraudulent behaviors. This, in turn, can facilitate the development of fraud detection systems that are more adaptable and capable of anticipating fraudulent behavior.

References

[1] A. H. Alhazmi and N. Aljehane, "A survey of credit card fraud detection use machine learning," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*. IEEE, 2020, pp. 1–6.

[2] "Consumer sentinel network," https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

[3] J. Egan, "Credit Card Fraud Statistics — Bankrate — bankrate.com," https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/, 2023.

[4] "Card-present fraud definition," https://www.investopedia.com/terms/c/cardpresent-fraud.asp, (Accessed on 10/16/2023).

[5] "6 common types of credit card fraud and how to avoid them," https://www.cardratings.com/financial-literacy/fraud/6-common-types-of-credit-card-fraud-and-how-to-avoid-them.html, (Accessed on 10/16/2023).

[6] "How Do Hackers Steal Credit Card Information? — TechTarget — techtarget.com," https://www.techtarget.com/whatis/feature/How-do-cybercriminals-steal-credit-card-information, [Accessed 27-09-2023].

[7] "Credit Card Data Breach: What It Is amp; Ways To Prevent It — Chase — chase.com," https://www.chase.com/personal/credit-cards/education/basics/credit-card-data-breach, [Accessed 27-09-2023].

[8] "Credit card fraud detection: Everything you need to know," https://www.inscribe.ai/fraud-detection/credit-fraud-detection, (Accessed on 10/16/2023).

[9] "What's credit card fraud detection? — capital one," https://www.capitalone.com/learn-grow/privacy-security/credit-card-fraud-detection/, (Accessed on 10/16/2023).

[10] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2019, pp. 488–493.

[11] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: a review of anomaly detection techniques and recent advances," *Expert systems With applications*, vol. 193, p. 116429, 2022.

[12] P. Kumar and F. Iqbal, "Credit card fraud identification using machine learning approaches," in *2019 1st International conference on innovations in information and communication technology (ICIICT)*. IEEE, 2019, pp. 1–4.

[13] V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," *Procedia computer science*, vol. 165, pp. 631–641, 2019.

[14] K. K. Tripathi and M. A. Pavaskar, "Survey on credit card fraud detection methods," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 11, pp. 721–726, 2012.

[15] H. Paruchuri, "Credit card fraud detection using machine learning: A systematic literature review," *ABC Journal of Advanced Research*, vol. 6, no. 2, pp. 113–120, 2017.

[16] V. Patil and U. K. Lilhore, "A survey on different data mining & machine learning methods for credit card fraud detection," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 5, pp. 320–325, 2018.

[17] X. Zhou, S. Cheng, M. Zhu, C. Guo, S. Zhou, P. Xu, Z. Xue, and W. Zhang, "A state of the art survey of data mining-based fraud detection and credit scoring," in *MATEC Web of Conferences*, vol. 189. EDP Sciences, 2018, p. 03002.

[18] S. Mehndiratta and K. Gupta, "Credit card fraud detection techniques: a review," *Int. J. Computer Sci. Mobile Computing*, vol. 8, no. 8, pp. 43–49, 2019.

[19] S. J. Omar, K. Fred, and K. K. Swaib, "A state-of-the-art review of machine learning techniques for fraud detection research," in *Proceedings of the 2018 International Conference on Software Engineering in Africa*, 2018, pp. 11–19.

[20] I. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," in *Proceedings of the 4th international conference on smart city applications*, 2019, pp. 1–4.

[21] J. Singla *et al.*, "A survey of deep learning based online transactions fraud detection systems," in *2020 International Conference on Intelligent Engineering and Management (ICIEM)*. IEEE, 2020, pp. 130–136.

[22] C. G. Tekkali and J. Vijaya, "A survey: methodologies used for fraud detection in digital transactions," in *2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 2021, pp. 1758–1765.

[23] A. K. Rai and R. K. Dwivedi, "Fraud detection in credit card data using machine learning techniques," in *Machine Learning, Image Processing, Network Security and Data Sciences: Second International Conference, MIND 2020, Silchar, India, July 30-31, 2020, Proceedings, Part II 2*. Springer, 2020, pp. 369–382.

[24] T. Amarasinghe, A. Aponso, and N. Krishnarajah, "Critical analysis of machine learning based approaches for fraud detection in financial transactions," in *Proceedings of the 2018 International Conference on Machine Learning Technologies*, 2018, pp. 12–17.

[25] R. R. Popat and J. Chaudhary, "A survey on credit card fraud detection using machine learning," in *2018 2nd international conference on trends in electronics and informatics (ICOEI)*. IEEE, 2018, pp. 1120–1125.

[26] A. K. Rai and R. K. Dwivedi, "Fraud detection in credit card data using unsupervised machine learning based scheme," in *2020 international conference on electronics and sustainable communication systems (ICESC)*. IEEE, 2020, pp. 421–426.

[27] S. Vimal, K. Kayathwal, H. Wadhwa, and G. Dhama, "Application of deep reinforcement learning to payment fraud," *arXiv preprint arXiv:2112.04236*, 2021.

[28] B. A. Sourabh, "A review of credit card fraud detection techniques," in *Recent Innovations in Computing*. Springer, 2022, p. 485—496.

[29] Z. Zojaji, R. E. Atani, A. H. Monadjemi *et al.*, "A survey of credit card fraud detection techniques: Data and technique oriented perspective," *arXiv preprint arXiv:1611.06439*, 2016.

[30] K. Gu, "Deep learning techniques in financial fraud detection," in *Proceedings of the 7th International Conference on Cyber Security and Information Engineering*, 2022, pp. 282–286.

[31] A. S. Gorte, S. Mohod, R. Keole, T. Mahore, and S. Pande, "Credit card fraud detection using various machine learning and deep learning approaches," in *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2022, Volume 3*. Springer, 2022, pp. 621–628.

[32] M. Ashraf, M. A. Abourezka, and F. A. Maghraby, "A comparative analysis of credit card fraud detection using machine learning and deep learning techniques," in *Digital Transformation Technology: Proceedings of ITAF 2020*. Springer, 2022, pp. 267–282.

[33] R. Asha and S. K. KR, "Credit card fraud detection using artificial neural network," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35–41, 2021.

[34] N. Shirodkar, P. Mandrekar, R. S. Mandrekar, R. Sakhalkar, K. C. Kumar, and S. Aswale, "Credit card fraud detection techniques–a survey," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*. IEEE, 2020, pp. 1–7.

[35] Y. Lucas and J. Jurgovsky, "Credit card fraud detection using machine learning: A survey," *arXiv preprint arXiv:2010.06479*, 2020.

[36] M. Alamri and M. Ykhlef, "Survey of credit card anomaly and fraud detection using sampling techniques," *Electronics*, vol. 11, no. 23, p. 4003, 2022.

[37] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University-Computer and Information Sciences*, 2022.

[38] A. M. Fayyomi, D. Eleyan, and A. Eleyan, "A survey paper on credit card fraud detection techniques," *International Journal of Scientific & Technology Research*, vol. 10, no. 09, 2021.

[39] T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, "Deep learning methods for credit card fraud detection," *arXiv preprint arXiv:2012.03754*, 2020.

[40] T. R. Pillai, I. A. T. Hashem, S. N. Brohi, S. Kaur, and M. Marjani, "Credit card fraud detection using deep learning technique," in *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*. IEEE, 2018, pp. 1–6.