

A Survey of Credit Card Fraud Detection using Machine Learning

Miss. Jui Sunil Udgate¹ Miss. Prachi Sunil Shinde² Miss. Bhagyashri Dayanand Sorate³ Miss. Aishvarya Sanjaykumar Hodagepatil⁴ Prof. A. B. Shikalgar⁵

^{1,2,3,4,5}Department of Computer Science and Engineering

^{1,2,3,4,5}Dr. J. J. Magdum College of Engineering, Jaysingpur, India

Abstract— It is vital that credit card companies are able to identify fraudulent credit card transactions so that customers are not charged for items that they did not purchase. Such problems can be tackled along with Machine Learning. This project intends to illustrate the modelling of a data set using machine learning with Credit Card Fraud Detection. The Credit Card Fraud Detection Problem includes modelling past credit card transactions with the data of the ones that turned out to be fraud. This model is then used to recognize whether a new transaction is fraudulent or not. Our objective here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications. Credit Card Fraud Detection is a typical sample of classification. In this process, we have focused on analysing and pre-processing data sets as well as the deployment of multiple anomaly detection algorithms such as Naïve Bayes, K-Nearest Neighbours, Logistic Regression and Support Vector Machine Model. Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. Since credit card is the most popular mode of payment, the number of fraud cases associated with it is also rising. In this paper, the survey on the present techniques available for detecting fraud in credit card is presented as a review paper. Fraud detection involves identifying fraud as quickly as possible once it has been done. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. The transaction is classified as normal, abnormal or suspicious depending on this initial belief. Once a transaction is found to be suspicious, belief is further strengthened or weakened according to its similarity with fraudulent or genuine transaction history using Bayesian learning. This paper investigates and checks the performance of Decision tree, Random Forest, SVM and logistic regression on highly skewed credit card fraud data. Dataset of credit card transactions is sourced from European cardholders containing 284,786 transactions. These techniques are applied on the raw and pre-processed data. The performance of the techniques is evaluated based on accuracy, sensitivity, specificity, precision. The results indicate about the optimal accuracy for logistic regression, decision tree, Random Forest and SVM classifiers are 97.7%, 95.5% and 98.6%, 97.5% respectively.

Keywords: Credit Card, Fraud Detection, Machine Learning

I. INTRODUCTION

Credit card plays a very important role in today's economy. It becomes an unavoidable part of household, business and global activities. Although using credit cards provides enormous benefits when used carefully and responsibly, significant credit and financial damages may be caused by fraudulent activities. Many techniques have been proposed to confront the growth in credit card fraud. However, all of these techniques have the same goal of avoiding the credit card fraud; each one has its own drawbacks, advantages and

characteristics. In this paper, after investigating difficulties of credit card fraud detection, we seek to review the state of the art in credit card fraud detection techniques, datasets and evaluation criteria. The advantages and disadvantages of fraud detection methods are enumerated and compared. Furthermore, a classification of mentioned techniques into two main fraud detection approaches, namely, misuses (supervised) and anomaly detection (unsupervised) is presented.

A. Types of fraud

The types of frauds considered in this paper are Credit card frauds, Telecommunication frauds, Computer intrusions, Bankruptcy fraud, Theft fraud/counterfeit fraud, Application fraud, Behavioural fraud.

- 1) Credit Card Fraud: Credit card fraud is divided into two types:
 - Offline fraud-Offline fraud is done by using a stolen physical card at any place.
 - On-line fraud-On-line fraud is committed over internet, phone, online shopping or when the card holder is not present.
- 2) Telecommunication Fraud: The use of telecommunication services to commit other forms of fraud. Consumers, businesses and communication service provider are the victims.
- 3) Computer Intrusion: Intrusion is defined as 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 knows the layout of the system.
- 4) 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.
- 5) Theft Fraud/ Counterfeit Fraud: In this section, the focus is on theft and counterfeit fraud, which are related to one other. Theft fraud refers to the other person who is not the owner of the card.
- 6) Application Fraud: When any people apply for a credit card with false information then it 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) Internal Fraud: Banking sector allows their employees to access customer data. The data is the same information needed to access online banking to customer accounts. So the fraud can be done easily by an employee.

At the current state of the world, financial organizations expand the availability of financial facilities by employing of innovative services such as credit cards,

Automated Teller Machines (ATM), internet and mobile banking services. Besides, along with the rapid advances of e-commerce, the use of credit card has become a convenience and necessary part of financial life. Credit card is a payment card supplied to customers as a system of payment.

There are lots of advantages in using credit cards such as:

- 1) Ease of purchase: Credit cards can make life easier. They allow customers to purchase on credit in arbitrary time, location and amount, without carrying the cash. Provide a convenient payment method for purchases made on the internet, over the telephone, through ATMs, etc.
- 2) Keep customer credit history: Having a good credit history is often important in detecting loyal customers. This history is valuable not only for credit cards, but also for other financial services like loans, rental applications, or even some jobs. Lenders and issuers of credit mortgage companies, credit card companies, retail stores, and utility companies can review customer credit score and history to see how punctual and responsible customers are in paying back their debts.
- 3) Protection of Purchases: Credit cards may also offer customers, additional protection if the purchased merchandise becomes lost, damaged, or stolen. Both the buyer's credit card statement and company can confirm that the customer has bought if the original receipt is lost or stolen. In addition, some credit card companies provide insurance for large purchases.

Credit card generally refers to a card that is assigned to the customer (cardholder), usually allowing them to purchase goods and services within credit limit or withdraw cash in advance. Credit card provides the cardholder an advantage of the time, i.e., it provides time for their customers to repay later in a prescribed time, by carrying it to the next billing cycle. Credit card frauds are easy targets. Without any risks, a significant amount can be withdrawn without the owner's knowledge, in a short period. Fraudsters always try to make every fraudulent transaction legitimate, which makes fraud detection very challenging and difficult task to detect.

In 2017, there were 1,579 data breaches and nearly 179 million records among which Credit card frauds were the most common form with 133,015 reports, then employment or tax-related frauds with 82,051 reports, phone frauds with 55,045 reports followed by bank frauds with 50,517 reports from the statics released by FTC

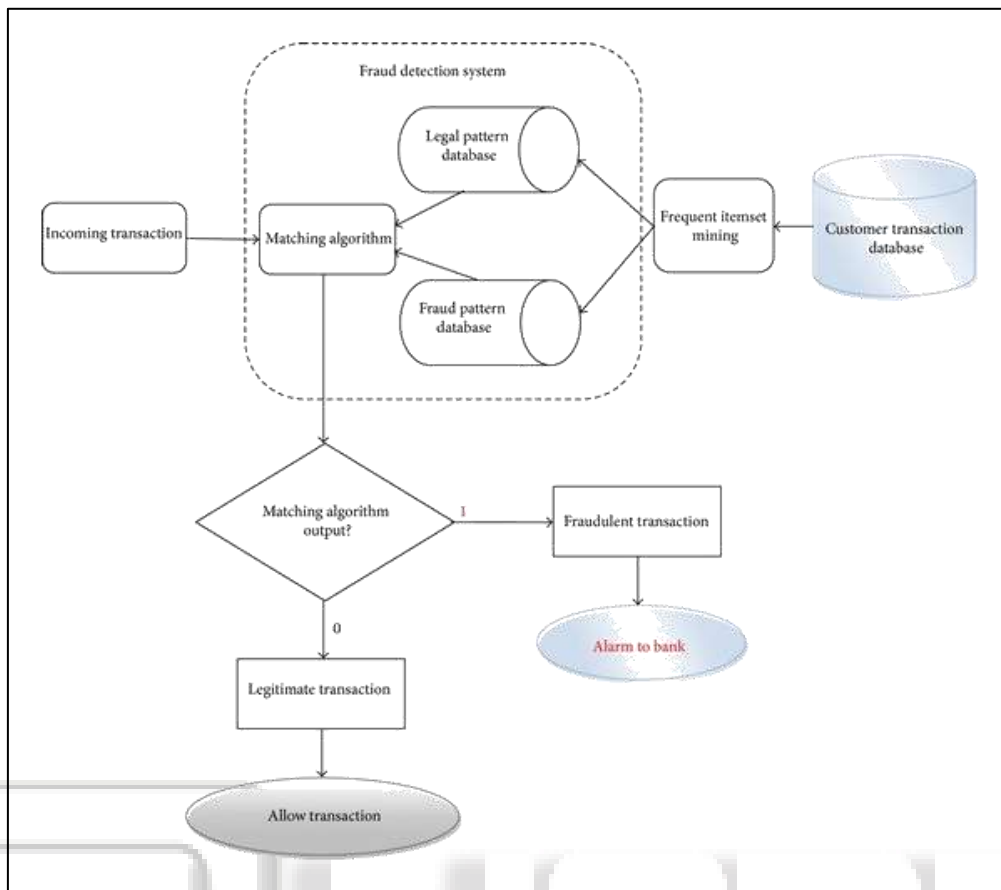
With different frauds mostly credit card frauds, often in the news for the past few years, frauds are in the top of mind for most the world's population. Credit card dataset is highly imbalanced because there will be more legitimate transaction when compared with a fraudulent one.

As advancement, banks are moving to EMV cards, which are smart cards that store their data on integrated circuits rather than on magnetic stripes, have made some on-card payments safer, but still leaving card-not-present frauds on higher rates.

B. Difficulties of Credit Card Fraud Detection:

Fraud detection systems are prone to several difficulties and challenges enumerated bellow. An effective fraud detection technique should have abilities to address these difficulties in order to achieve best performance.

- 1) Imbalanced data: The credit card fraud detection data has imbalanced nature. It means that very small percentages of all credit card transactions are fraudulent. This cause the detection of fraud transactions very difficult and imprecise.
- 2) Different misclassification importance: in fraud detection task, different misclassification errors have different importance. Misclassification of a normal transaction as fraud is not as harmful as detecting a fraud transaction as normal. Because in the first case the mistake in classification will be identified in further investigations.
- 3) Overlapping data: many transactions may be considered fraudulent, while actually they are normal (false positive) and reversely, a fraudulent transaction may also seem to be legitimate (false negative). Hence obtaining low rate of false positive and false negative is a key challenge of fraud detection systems.
- 4) Lack of adaptability: classification algorithms are usually faced with the problem of detecting new types of normal or fraudulent patterns. The supervised and unsupervised fraud detection systems are inefficient in detecting new patterns of normal and fraud behaviours, respectively.
- 5) Fraud detection cost: The system should take into account both the cost of fraudulent behaviour that is detected and the cost of preventing it. For example, no revenue is obtained by stopping a fraudulent transaction of a few dollars.



II. LITERATURE SURVEY

The fraud detection is a complex task and there is no system that correctly predicts any transaction as fraudulent. The properties for a good fraud detection system are:

- 1) Should identify the frauds accurately.
- 2) Should detect the frauds quickly.
- 3) Should not classify a genuine transaction as fraud.

Fraudulent transactions act as the illegal activities which are meant to generate personal or financial profit. It is an intentional act that is criminal with an intention to make financial profit. Multiple Supervised and Semi-Supervised machine learning techniques are used for fraud detection, but we aim is to overcome three main challenges with card frauds related dataset i.e., strong class imbalance, the inclusion of labelled and unlabelled samples, and to increase the ability to process a large number of transactions.

Different Supervised machine learning algorithms like Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression and SVM are used to detect fraudulent transactions in real-time datasets. Two methods under random forests are used to train the behavioural features of normal and abnormal transactions. They are Random-tree-based random forest and CART-based. Even though random forest obtains good results on small set data, there are still some problems in case of imbalanced data. The future work will focus on solving the above-mentioned problem. The algorithm of the random forest itself should be improved.

Performance of Logistic Regression, K-Nearest Neighbour, and Naïve Bayes are analysed on highly skewed

credit card fraud data where Research is carried out on examining meta-classifiers and meta-learning approaches in handling highly imbalanced credit card fraud data. Through supervised learning methods can be used there may fail at certain cases of detecting the fraud cases. A model of deep Auto-encoder and restricted Boltzmann machine (RBM) that can construct normal transactions to find anomalies from normal patterns. Not only that a hybrid method is developed with a combination of Ada boost and Majority Voting methods

There are a number of literature or research papers available on this domain in the public platform. A detailed survey study conducted by Clifton Phua and his interns suggested methodologies used in this domain are data mining applications, Fraud detection, adversarial detection. In another research paper Suman threw lights that techniques like supervised and unsupervised learning for fraud detection. Indeed these methods were very effective and efficient in some areas of the domain but they failed to give a permanent solution to the fraud detection in credit cards. In a similar research paper by Wen-Fang Yu and Na Wang, in which they used outlier mining, outlier detection mining and Distance sum algorithm to predict fraud in an experiment conducted on the credit card data of some particular commercial banks.

Outlier mining is a technique of data mining which is mostly applied in the fields related to finance or internet. It detects the fields which are not genuine. In this technique we take fields of customers behaviour and on the basis of that we determine the distance between the observed value of the field and the predetermined value. There is some literature which suggests a completely new perspective to detect fraud. In case of fraudulent transactions, there have been some

studies to make the alert feedback interaction more efficient. Whenever a fraudulent transaction is encountered an alert will be generated and sent to the authorised server system which in return will deny the transaction. One of the many other aspects of Artificial Genetic Algorithm is an advancement to deal with the problem in a totally different aspect. This method resulted in more accurate fraud detection and less number of false alerts.

III. METHODOLOGY

Our paper suggests an aspect of latest machine learning algorithms to detect fraudulent or anomalous events commonly called outliers.

We have used a dataset provided by Kaggle, this dataset comprises the transaction records of the European card holders in the year 2013. Inside the dataset there are 31 columns out of which 30 are used as features and the remaining 1 column is used as class. Our features include Time, Amount and Number of transactions.

First of all, we obtained our dataset from Kaggle, a data analysis website which provides datasets. Inside this dataset, there are 31 columns out of which 28 are named as v1-v28 to protect sensitive data. The other columns represent Time, Amount and Class. Time shows the time gap between the first transaction and the following one. Amount is the amount of money transacted. Class 0 represents a valid transaction and 1 represents a Fraudulent one.

We have plotted a graph which shows the inconsistency in the dataset. Kindly refer to figure for the same. This graph shows that the number of fraud transactions is very less as compared to authorized transactions.

To determine the pattern of the fraudulent transactions we have plotted three graphs between: Number of transactions vs Time, Number of transactions vs amount, Amount vs Time.

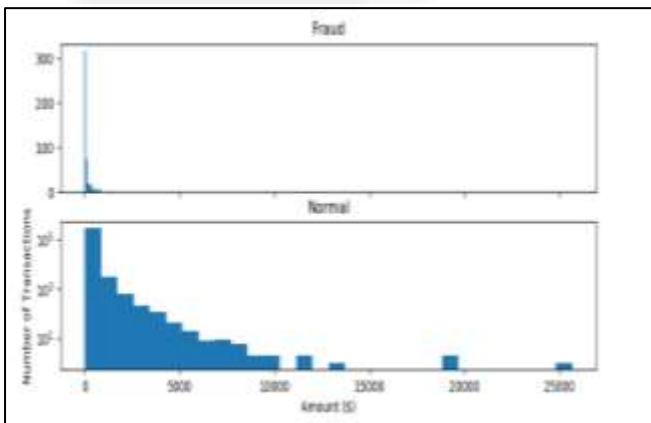


Fig. 3.1: Amount vs Number of transactions.

This graph shows the relation between Number of transactions and Amount

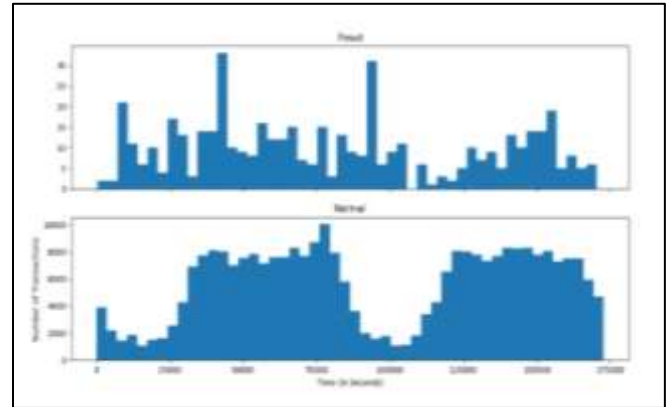


Fig. 3.2: Time vs Number of Transactions

This graph shows the relation between Number of transactions and Time.

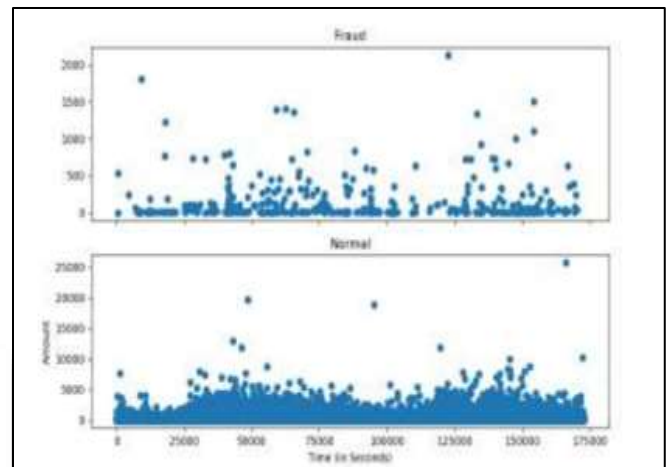
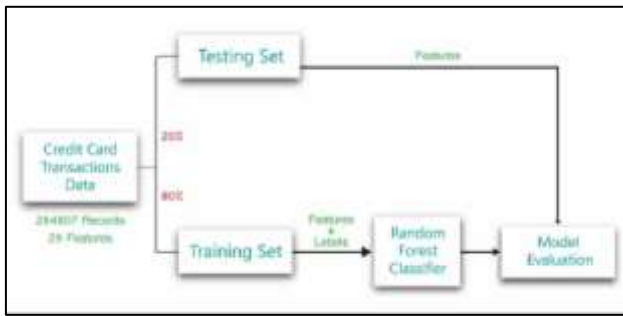


Fig. 3.3: Time vs Amount

This graph shows the relation between Amount and Time. These graphs give us a correlation between all the features of the dataset which will help us to detect an anomaly.

IV. NAÏVE BAYES

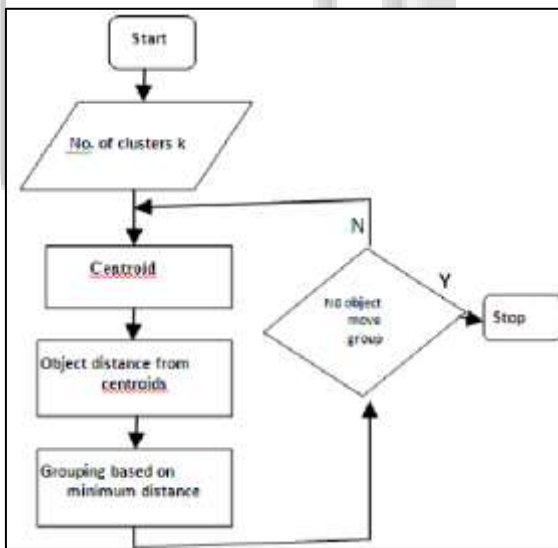
Naïve Bayes (NB) is a supervised machine learning method that uses a training dataset with known target classes to predict the future or any incoming instance's class value. Naïve Bayes classifier is noted as a powerful probabilistic method that exploits class information from training dataset to predict the class of future instances. Naïve Bayes method assumes that the presence or absence of any attribute of a class variable is not related to the presence or absence of any other attributes. This technique is named "naïve" because it naïvely assumes independence of the attributes. The classification is done by applying "Bayes" rule to calculate the probability of the correct class. Despite their naïve design and oversimplified assumptions, Naïve Bayes classifiers have good performance in many complex real world datasets.



V. K-NEAREST

K-nearest is the most simple and efficient method to cluster the data. Initially, the numbers of cluster K, and Centroid values are obtained. Any random objects as the initial Centroid or the first K objects can also serve as the initial Centroid. This technique is a non-hierarchical method; initially it takes the number of objects equal to the final required number of clusters.

- 1) Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.
- 2) Assign each object to the group that has the closest centroid.
- 3) When all objects have been assigned, recalculate the positions of the K centroids.
- 4) Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.



VI. LOGISTIC REGRESSION

The two data mining approaches, are support vector machines and random forests, together with the well-known logistic regression, as part of an attempt to detect the credit card fraud. It is well-understood, easy to use, and it is most commonly used for data-mining. Thus it provides a useful baseline for comparing performance of newer methods.

Supervised learning methods for fraud detection face two challenges. They are:

- 1) The unbalanced class sizes of legitimate and fraudulent transactions, with legitimate transactions far outnumbering fraudulent ones.
- 2) The second is to develop supervised models for fraud that can arise from potentially undetected fraud transactions, leading to mislabelled cases in the data to be used for building the model.

For the purpose of the above problems, the fraudulent transactions are those specifically identified by the institutional auditors as those that caused an unlawful transfer of funds from the bank sponsoring the credit cards. These transactions were observed to be fraudulent expose. The study is based on real-life data of transactions from an international credit card operation.

Metrics	Classifiers				
	Logistic Regression	SVM	Decision	Tree	Random Forest
Accuracy	0.977	0.975	0.955		0.986
Sensitivity	0.975	0.973	0.955		0.984
Specificity	0.923	0.912	0.878		0.905
precision	0.996	0.996	0.995		0.997

A. Support Vector Machine:

Support Vector Machines (SVMs) have developed from Statistical Learning Theory. They have been widely applied to fields such as character, handwriting digit and text recognition, and more recently to satellite image classification. SVMs, like ANN and other nonparametric classifiers have a reputation for being robust. SVMs function by nonlinearly projecting the training data in the input space to a feature space of higher dimension by use of a kernel function. This results in a linearly separable dataset that can be separated by a linear classifier. This process enables the classification of datasets which are usually nonlinearly separable in the input space. The functions used to project the data from input space to feature space are called kernels (or kernel machines), examples of which include polynomial, Gaussian (more commonly referred to as radial basis functions) and quadratic functions. Each function has unique parameters which have to be determined prior to classification and they are also usually determined through a cross validation process.

Support Vector Machines (SVM) is another classification algorithm that classifies data into one category or the other by using hyperplanes based on the training data. SVM essentially creates a model such that it finds the widest possible margins and thus the optimal hyperplane. SVM creates a separating hyperplane by transforming the data into higher dimensions where the data is separable using the kernel trick.

VII. FUTURE REFERENCES

While we couldn't reach our goal of 100% accuracy in fraud detection, we did end up creating a system that can, with enough time and data, get very close to that goal. As with any such project, there is some room for improvement here. The very nature of this project allows for multiple algorithms to be integrated together as modules and their results can be combined to increase the accuracy of the final result. This model can further be improved with the addition of more algorithms into it. However, the output of these algorithms needs to be in the same format as the others. Once that condition is satisfied, the modules are easy to add as done in

the code. This provides a great degree of modularity and versatility to the project. More room for improvement can be found in the dataset. As demonstrated before, the precision of the algorithms increases when the size of dataset is increased. Hence, more data will surely make the model more accurate in detecting frauds and reduce the number of false positives. However, this requires official support from the banks themselves.

VIII. CONCLUSION

Credit card fraud is without a doubt an act of criminal dishonesty. This article has listed out the most common methods of fraud along with their detection methods and reviewed recent findings in this field. This paper has also explained in detail, how machine learning can be applied to get better results in fraud detection along with the algorithm, pseudocode, explanation its implementation and experimentation results. While the algorithm does reach over 99.6% accuracy, its precision remains only at 28% when a tenth of the data set is taken into consideration. However, when the entire dataset is fed into the algorithm, the precision rises to 33%. This high percentage of accuracy is to be expected due to the huge imbalance between the number of valid and number of genuine transactions.

REFERENCES

- [1] Jiang, Changjun et al. "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism." *IEEE Internet of Things Journal* 5 (2018): 3637-3647.
- [2] Pumsirirat, A. and Yan, L. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. *International Journal of Advanced Computer Science and Applications*, 9(1).
- [3] Mohammed, Emad, and Behrouz Far. "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study." *IEEE Annals of the History of Computing*, IEEE, 1 July 2018.