International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.8, Issue.6, June 2020 E-ISSN: 2347-2693

Real-time Transactions Fraud Detection Via Machine Learning Techniques : A Review

Kapil Dev Tripathi[1*], Vikas Singh Rajput[2]

[1,2] Department of CSE, ShriRam College of Engineering & Management, Gwalior, India

**Corresponding Author: kapil.dev.tripathi24@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v8i6.5156 | Available online at: www.ijcseonline.org

Received: 25/May/2020, Accepted: 20/June/2020, Published: 30/June/2020

***Abstract*—** This paper represents survey of various techniques utilized in Credit Card Fraud Detection (CCFD) mechanisms. There are many new and modern techniques depending upon Neural Network (NN) and Artificial Intelligence (AI), Data mining (DM), Artificial Immune System (AIS), Bayesian Network (BN), Fuzzy Logic Based System, Decision Tree (DT), K- nearest neighbor (KNN) algorithm, Support Vector Machine (SVM), Machine Learning (ML), Genetic Programming (GP) etc., which has developed fraudulent transactions to detect various credit card. Various techniques for the FD system have been explained. The powerful FD system, which detects the fraud, but also detects it in a precise manner, is needed in order to stop these frauds. They also need to make our systems learn about or adapt to future new methods of fraud from past frauds. The concept of CC fraud, or its different types, has been introduced in this paper.

***Keywords*—** Real-time Fraud Detection, Fraud Detection System (FDS), Machine Learning (ML), CCFD Techniques, CCF.

I. INTRODUCTION

FD automates and reduces manual feature of screening / checking procedure as part of general fraud control. In industry & government, this field has become one of the most established applications for DM. The legitimacy of the intention behind the application and transaction is impossible to be absolutely certain. Given truth, Mathematical algorithms are used to tease probable evidence of fraud from available data as best cost-effective option. The term fraud refers to exploitation of a clear substantive impact in a financial organization system. In a competitive market, fraud will become a key business problem when preventive practices become widespread and are not safe [1]. The identification of fraud is a very difficult task, as it is completely different in nature and has millions of methods. The traditional methods of data analysis were therefore used for a long time for detecting fraud. We are demanding complex and time-consuming tasks that deal with various fields of knowledge such as business, finance, economics and law. In general, in appearance or material, fraud instances can be similar but are not typically identical. The identification of fraud is therefore very difficult. Introduce various techniques or methods for detecting them here. Naive Bayes (NB), BN, NN, Neural perceptron network, AIS, CCFD, DT etc. These are the different tools and approaches used to identify corporate fraud, banks, credit card companies, etc. In this text, we present the different techniques and benefits, as well as the various algorithms and systems which are faster than before when fraud is detected [2].

Credit Card (CC) use has now become a common scenario even in developing countries. People use this for the shop, payment of bills or transactions online. But, with the number of CC users increasing. Loss of billions of dollars on credit Card fraud (CCF) occurs globally. Fraud can be defined as any activity to get financial gains in any manner without knowledge of cardholder or issuer bank. CC abuse can be completed with lost or stolen cards in many ways, by producing counterfeit and fake cards, Cloning of original site, By erasing and changing magnetic strip on card containing information from user, By skimming and stealing merchant's data side, FD identifies fraud among thousands of genuine individuals, That actually puts challenge forward. It is important to develop efficient models only in their first stage in order to combat fraud in the continuing advancement of fraudulent strategies; you can stop before you can do it. Nonetheless, main challenge in developing model is very small no. of fake transactions, and it is therefore very difficult to identify effective and efficient fraudulent offers [3].

ML is the paradigm that can refer to previous (in this case past) learning so that future results can be improved. Automatic learning methods are the only focus of this field. A phenomenal outcome when Computer Science & Statistics joined forces was learning to modify and enhance algos depends upon past "experiences" repeatedly except external assistance from human ML. CS concentrates on building machines that solve specific issues and tries to classify possibilities to solve issues. Most important technique that Statistics basically employs is data inference, Hypothesis modeling & reliability measurement

of conclusion. The little bit different, but partly dependent on both, is the defining idea of ML. while CS focus on manually programming computers, when new data are exposed on the basis of initial learning strategy, the re-program problem is addressed by ML. The statistics alternatively, focus on data inference and probability, ML contains further issues about efficiency & feasibility of data processing algorithms & architectures, compounding several learning tasks with one compact or performance measure [4].

The purpose of the contribution to explain or correctly interpret the primary contribution made.

These contributions are:

1. It provide clearly articulate the ways in which the credit fraud has occurred;
2. On the basis of earlier researches provide a real time CCFD system; and
3. To define what the causes of these frauds happening are, reduces these by various machine learning algorithm and what are the outcomes.

Rest of the paper is organized as follows, Section I contains introduction of CCFD by using ML. Section II contains the FD system, Section III contain the credit card fraud and some techniques of credit card fraud, Section IV contain the real time fraud detection system and how to work it, section V explain the related work of credit card fraud, and Section VIII concludes review on credit card fraud research work with future directions.

II. FRAUD DETECTION SYSTEM

Aim of Fraud Detection system (FDS), therefore, is to pre-determine all transactions, regardless of preventive measures, to be fraudulent, and to identify transactions as fraudulent, following fraudulent as soon as possible. Ones after fraudsters have begun to make fake transactions as quickly as possible. CCFD is a massive & trendy problem. Various FD systems evaluate transactions & generate suspicion score (usually probability from 0 to 1), This indicates likelihood of fraudulent transaction. These scores are determined by methods used for model(s) creation in FD systems. These equivalent values are utilized to distinguish among fraudulent transactions from legitimate ones by means of an advanced threshold value. [5].

A. *Fraud Detection Cases*

1) *Credit Card Fraud Detection:* This model adopts uncontrolled learning. This model detects variations in behavior or unusual transactions without understanding of fraudulent and non-fraudulent transactions in advance. Such methods form a basis of the standard behavioral representation used to identify results that indicate extreme deviations from this baseline. The approach is unregulated to identify previously unknown types of fraud, but substandard tests are used to detect them. In the outlier detection approach using a supervised learning system, it is only useful to detect prior swindles and to classify fraudulent transactions accurately. This technique's biggest shortcoming is that only pre-revealed fraud can be observed. Abnormal spending activity and volume of transactions.
2) *Telecommunication Fraud Detection:* The action of different users is modified sophisticatedly. The user profiles of network computers are unique. It is therefore used widely in fraud detection. Neural networks will cut operating costs significantly. Together with the controlled & unmonitored method of the European Commission, the ASPECT project explored the practicality of a neural and rule-based approach to the instigation of mail tickets. Three ideas based on toll tickets (call records for billing purposes) were presented. Next, the supervised nerve network for feedback that classifies subscribers by observing a non-linear discriminatory function using digest statistics. Second, the Gaussian Mixing Model Density Assessment detects all abnormalities of past behavior by using them to sculpt all subscribers ' previous behavior. Second, the Bayesian networks are used to describe probabilistic models described by the actions of subscribers.
3) *Online Auction Fraud Detection:* Online auction is gaining immense popularity by creating an environment for the fair exchange of goods. While there are rapidly growing numbers of online vendors and buyers, this modern business medium is challenging an essential challenge-the auction fraud. Sellers & buyers alike can participate for their own benefit in auction fraud. Pre-auction & post-auction frauds don't rely much on the online prevention and detection system because it involves offline actions. In the event of fraud in the auction, on the other hand, it can occur without direct physical proof and is even more nasty to have the victims unable to perceive it. The nature of the detection of auction fraud has intrigued much less than the previously fascinated policymakers and scholars, while pre-and post-auction frauds.
4) *Computer Intrusion Detection:* A review of operating system audit data becomes the basis for many intrusion detection system operations. The historical operation record on a machine that is recorded in a file is known as an audit report. Improved intrusion detection system monitoring is provided by maintaining cumulative audit statistics. Categorical classification focused on an intrusion detection model Misuse Prevention & Anomaly Detection [6].

III. CREDIT CARD FRAUD

CC is the most frequently used payment method in online transactions and gradually there is an increase in fraudulent transactions as well. The intention behind these kinds of fraudulence may be obtaining goods except paying, / unauthorized funds by an account. Generally, people associate the crime of credit card fraud with ID theft. Now the ID theft decreased into a percentage. A survey proved

that about 0.1% fraudulence is by credit card. This has resulted in huge financial losses [7].

Fraud acts as a deceptive or criminal dissatisfaction that results in income for finance or personnel. CCF, therefore, is illegal or exhaustive use of a card or unusual behavior of transaction. The bank, merchants & consumers were affected by so many frauds. Some of them appear in the following:

- Mails inception of recently issued cards.
- Copying/ replicating of card details by cloned websites.
- Phishing where credit card numbers & passwords are stolen like e-mails, etc.
- Triangulation Fraudster makes legitimate websites & advertisements for selling products at significantly lower rates in this kind of fraud. Unaware users attract & transact online on these pages. You supply your card details for the purchase of those items. Then fraudsters make genuine transactions by using this card information [8].

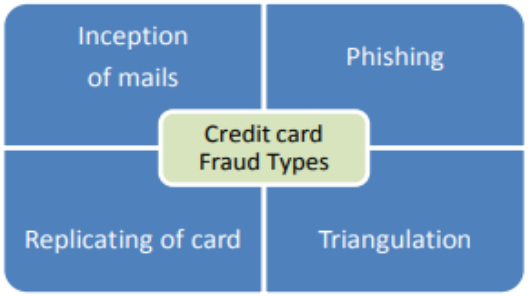

Figure 1. General Types of Credit Card Fraud

A. Types of CCF

1) *Application Frauds:* If fraudster manages the app process by manipulating confidential user details such as password & username and opening a fake account. This usually takes place in response to the abuse of identity. Where fraudster is in name of cardholder applying for a refund or new CC. Fraudsters rob documents of their fake application or prove them.
2) *Electronic and Manual Credit Card Imprints:* If fraud skims details put on card's magnetic strip. Information is highly confidential, and fraudsters can in future usage it for fake transactions through access.
3) *CNP (Card Not Present):* Date of expiry for fraudster and no. of card account, Except for this true physical possession, a card may be used.
4) *Counterfeit Card Fraud:* Usually, this is tried during skimming. The magnetic swipe card has been counterfeit and contains all the data of the card. Counterfeit card is completely workable also may be utilized in future transactions.
5) *Lost and Stolen Card Fraud:* In situations where unique cardholder refuses to position his card, fraudsters can be held responsible for it and then transactions can be made by them. It is difficult to do this by computer because a pin number is needed; however, the fraudster can easily be transacted online.
6) *Card ID Theft:* Similar to computer frauds is this fraud. Through ID robbery, the fraudster gets information for using or opening a new card on the original identity. That is the hardest fraud to understand.
7) *Mail Non-Receipt Card Fraud:* If client requests the card all administrative formalities require a certain amount of time. If a fraudster intercepts in the middle of delivery, a card can be registered on your behalf and used for purchase this scam is also called fraud that has never been received.
8) *Account Takeover:* It is most common fraud types. Fraudster can obtain account details and several relevant documents from the original cardholder. You can then contact a company that has a CC and claim to be the original cardholder. They may give them proof as well, since they have all data as evidence, hacked or otherwise accessed. A duplicate card is then transmitted to a new or fake address, which criminals can use.
9) *False Merchant Sited:* It is the same as an attack by phishing, where a user is trapped in a counterfeit fraudster's website, which is much like a legitimate & established website. In order to encourage customers to buy products, this Website will offer several discounts. Once the transaction is made, all information about the transaction is collected as well as fraudster continues to exchange fraudulent data.
10) *Merchant Collusion:* When the dealer intentionally transmits appropriate cardholder data without cardholder being informed of this. Fraud detection is a complex computer function. There is a lot of parameters to choose from, to compile and also to identify and to decide on the success of every technique of detection of fraud. In addition, an operation can not merely be classified by existing systems as a fraud or as genuine one; it merely finds that the likelihood of transaction is a fraud based on an exhaustive examination of client behavior, their spending habits and analysis & observation of fraud previously committed [9].

B. Different Techniques of CCFD

They are all aware that any fake transaction is identical, and we can identify transactions as fake, functioning of which is described below by some pattern recognition method like Naïve Bayesian Network, ANN, DTs, Support Vector Machine (SVM), Fuzzy Logic Based Method, Hidden Markov Model (HMM), KNN.

1) *ANN:* It integrates human brain reasoning with computational power of the machine. Neurons are utilized as reference location and boundaries among neurons to determine contribution of every neuron to prior layer & outcome currently in neuron. It is aimed at identifying trends. Last year's data are entered in the network and then a new incoming transaction is known as fake or legitimate depending upon that data. [10].
2) *Decision Tree (DT):* A computational tool is prediction and classification. The result for each branch is shown in an internal node tree, showing a measure of a particular attribute, and every leaf node has class label (terminal node). It reciprocally divided a data set into

breath first greedy method (BFGM) or the depth-first greedy method (BFGM) & stops whilst each item has been allocated a particular class.

3) *Fuzzy Logic (FL):* It is used when values of facts are not secure, but are continuous. This is logic of multi-value. A transaction is characterized by certain rules as genuine or fraudulent.
4) *SVMs*: It is Supervised Learning Algo, where hyperplane dataset can divide the data into different classes. SVM is located for this hyperplane. There may be several hyperplanes and yet we are eager to obtain a best hyperplane. Support vectors are called nearest points to the hyperplane for different classes and those support vectors are utilized to calculating new data point classes. A new point of input into the hyperplanes is made and is then classified as class in which hyperplanes side falls into vector space.
5) *Bayesian Network (BN):* Bayes' conditional theorem is utilized & therefore is probabilistic approach used to automatically predict different events. It has nodes and edges. The probability of fraud or legal transaction is calculated on a predefined minimal & maximal value. For new incoming transaction, we can therefore see that probability of legal transaction is lower than defined minimum value, and greater than defined maximum value of fraud transact. Whether transaction is true is classified like fraud.
6) *K-Nearest Neighbour (KNN):* most common algorithms are regression and classification issues. Efficiency varies with 3 factors: distance metrics, distance rule and K value. Distance metrics show that nearest neighbors should be located to every data point. Distance rule allows us, by comparing the features by those of neighboring data points, for grouping new data points into a single category. We determine the dominant class and add this dominant class transaction in vicinity of each new transaction. [11].
7) *Hidden Markov Model (HMM):* The state with time changes, which is why the name is Markov. The conditions are therefore not directly observed. But something similar to them can be observed & we estimate the order of changes on the basis of this sequence of observations. After that, a new transaction is evaluated by means of our model and categorized as fraudulent, whether or not a cardholder with a threshold value varies with a common profile and behavior and therefore can not be evaluated in HMM states. [12].
8) *Logistic Regression (LR):* In the play against linear regression anomalies, LR is involved in the play where values above 1 & below 0. Given the regression of name, LR is utilized to predict binomial & multinomial outcome classification problems with the objective of estimating parameter coefficient values by using a sigmoid function. LR is for clustering that tests the attributes values when a transaction is in process and informs whether or not a transaction is to be made. [13].

IV. REAL-TIME FRAUD DETECTION SYSTEM

FD was done with transactions that already happened in bulk to use ML models. The results have been extremely difficult to track fraud as weeks or months later, In many cases, fraudsters have been able to, To make a lot more fraudulent purchases before being exposed. The efficiency of FD models is the real-time FD, The second is online shopping. It allows our system to FD in real-time. It alerts the bank about its accuracy rate and fraud pattern, making it easy for teams monitoring fraud to proceed without wasting time and money. CCFD in real-time is main contributions to this project. There are three main units of the real-time FD system; FRAUD DETECTION, API MODULE & DATA WAREHOUSE MODELS. All elements are simultaneously concerned in FD. Fraudulent transactions (frauds occur because of risky MCC) are classified into four types of fraud, Unknown web address, ISO Response Code, above $100 transaction) using 3 supervise learning classifiers. The API module transfers transactions in real-time between the FD model, GUI & data storage. Data Warehouse has been utilized to store live transactions, predicted results & further ML models. User can relate with GUIs to show real-time transactions FD system, Fraud alerts and historical data on the representation of fraud. When the FD model recognizes the transaction fraudulent, message to an API module will be sent. Afterwards, API module notifies end user of message or stores end-user feedback [14].

V. RELATED WORK

D. Varmedja et al. [2019] show multiple algorithms that may be used as fraud or real to identify transactions. In the study, the CCFD dataset was utilized. Due to the highly imbalanced data set, SMOTE technology for over-sampling was used. In addition, feature collection, as well as a dataset, is split into 2 sections, training data & test data. LR, NB, Random Forest (RF) and Multilayer Perceptron (MLP) were algorithms utilized in this experiment. Results demonstrate that every algorithm may be used with high precision to CCFD. The main aim is to measure loss of sensitive information about CC [15].

S. Mittal and S. Tyagi et al. [2019] In this study, a highly unbalanced dataset used commonly supervised & unsupervised ML algorithms for the order to detect CCF. Unsupervised ML algorithms have been found to manage skewness and to give the best results in classification. CC transactions are now a common place, as well as resulting frauds is also prevalent. Most popular forms of fraud detection (FD) is illegally collecting card data & utilize it for online shopping. It is impossible to identify such fraudulent transactions between thousands of regular transactions for CC companies & dealers [16].

S. Xuan et al. [2018] In order for criminals to steal CC information, certain people may utilize various technologies, like Phishing or Trojan. An efficient method

of detecting fraud is therefore critical because a criminal can detect fraud when a stolen card is used to consume. One way of doing this is to take full advantage of historical transaction information comprising regular transactions & fraud data to achieve normal / fraud-based behavior, and then to use them to check whether or not an operation is a fraud. In this work, behavior characteristics of normal & abnormal transactions were trained in 2 types of RFs. The aim of compare 2 RFs in scope & evaluate the quality of them in the detection of credit fraud. [17].

I. Benchaji et al. [2018] suggest a sampling technique, depends on K-means Clustering as well as GA, to enhance the classifying efficiency of Minority of CCF instances in imbalanced data set. To each group we utilize genetic algorithm (GA) to gather novel samples & build a precise FD classifier in each cluster we have used the K-means algorithm. Financial fraud was also dramatically increased with the increasing use of CC transactions, In the financial industry, it leads to a loss of large amounts. An effective method of FD has become a prerequisite for every bank to mitigate these losses [18].

R. R. Popat and J. Chaudhary et al. [2018] The main objective is to ensure safe & simple use of E-Banking through CC transactions. To identify CCF, different methods are depending on Deep learning, LR, NB, SVM, NN, Artificial Immunology, KNN, DM, DT, FL based system, GAs, etc. Data can also be detected. Digitalization is rapidly gaining popularity because E-commerce is used seamlessly, quickly & conveniently. The payment system was extremely rampant & easy. People prefer e-shopping & online payment, for convenience of time, transportation, etc. CCF is also rising, because of the huge amount of e-commerce usage. Fraudsters are trying to misuse cards or make online payments clear. It is thus very critical to overcome the actions of fraudsters [19].

J. O. Awoyemi et al. [2017] Performance is highly skewed CCF data of NB, KNN as well as LR are investigated. The credit card payments data set comes from 284.807 purchases in European card holders. The distorted results were obtained using a hybrid methodology for under-sampling & oversampling. 3 methods are used for raw & pre-processed information. Results showed optimal accuracy of 97.92 percent, 97.69 percent & 54.86 percent respectively for NB, KNN and LR classifications. The results show that KNN performs better than NB & LR techniques [20].

K. T. Hafiz [2016] Concentrate on developing scoring card depends on applicable evaluation criteria, attributes, & functionality to identify CCF using predictive analytics software supplier solutions. The scorecard lists five approaches introduced by predictive analytics companies in Canada on side by side basis. A list of CCF PAT solution provider problems, risks & constraints are illustrated in the following research findings. As part of fraud prevention programs to moderate CCF in the part of reducing financial losses and risk from reputation is the main objective of this work [21].

V. Mareeswari and G. Gunasekaran et al. [2016] suggested new algorithm together with the current algorithm. Limitation of existing systems is a matter of scalability problems, extremely imbalanced class as well as time constraints. More than identification is avoidance. Thus, by identifying fraud when applying for a card, the existing system avoided fraud by CC. Hybrid vector support (HSVM) & common and spike detection for detection of fraud application by cards overcome these limitations. HSVM is a method for identification and classification of patterns most used [22].

A. Agrawal et al. [2015] developed a method for CCFD. For every online & offline in the world today, CC can be approved. The techniques utilized are combined. Secondly, shopping conduct depends on the customer's type of products. Additionally, costs are based on the maximum amount of expended. Fraud is detected Thirdly, HMM is preserved in this technology and statistics are clustered from one particular user as well as from various fraud scenarios. For the estimation of threshold & accurate fraud, GA is utilized [23].

VI. CONCLUSION AND FUTURE SCOPE

Although several FD techniques are now available, none of them can completely detect fraud if they actually occur, Usually they detect it after the fraud occurs. In recent years, credit card usage has increased significantly. Fraud operations are also newly arriving in another way; there are more techniques introduced to detect the frauds. Main reason of this study is to know best technology to identify cases of fraud. This study is helpful to further early detect online fraud transactions and fraud card detection. Various machine learning techniques are very helpful to CCFD. For predicting such type of fraud a very effective model is real time CFD system which is designed to overcome this problem. From the observation of real time credit fraud detection system analysis and work it is clear that it can effectively predict and detect the credit card related fraud. However, there are various challenges are present. Remind these challenges this work will enhance by efficient method to accurately detection of fraud related to CC.

REFERENCES

[1] C. Phua, V. Lee, K. Smith and R. Gayler, "*A Comprehensive Survey of Data Mining-based Fraud Detection Research*", ArXiv, Vol. abs/1009.6119, pp. **1-14, 2007.**

[2] M. Arif and A. R. Dar, "*Survey on Fraud Detection Techniques Using Data Mining*", International Journal of u- and e-Service, Science and Technology, Vol.**8**, No.**3**, pp.**163-170, 2015**

[3] Y. Jain, "*A Comparative Analysis of Various Credit Card Fraud Detection Techniques*", International Journal of Recent Technology and Engineering (IJRTE), Vol.**7,** Issue-**5S2**, **2019.**

[4] K. Das, "*A Survey on Machine Learning: Concept, Algorithms, and Applications*", International Journal of Innovative Research

in Computer and Communication Engineering, Vol. **5**, Issue **2**, **2017.**

[5] A. Shen, R. Tong and Y. Deng, *"Application of Classification Models on Credit Card Fraud Detection*", International Conference on Service Systems and Service Management, **Chengdu**, pp. **1-4**, **2007.**

[6] P. Richhariya, Dr. P. K. Singh and E. Duneja, "*A Survey on Financial Fraud Detection Methodologies*", International Journal of Commerce, Business and Management (IJCBM), Vol. **1**, No.**1**, pp. **14-24, 2012.**

[7] Suman, "*Survey Paper on Credit Card Fraud Detection*", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. **3,** Issue **3**, **2014.**

[8] A. Shen, R. Tong and Y. Deng, *"Application of Classification Models on Credit Card Fraud Detection*", International Conference on Service Systems and Service Management, **Chengdu**, pp. **1-4**, **2007.**

[9] Y. Sahin and E. Duman, "*Detecting credit card fraud by ANN and logistic regression*", International Symposium on Innovations in Intelligent Systems and Applications, **Istanbul**, pp. **315-319**, **2011.**

[10] T. R. C.Sudha, "*Credit Card Fraud Detection In The Internet Using K Nearest Neighbor Algorithm*", IPASJ International Journal of Computer Science, Vol. **5**, No. **11**, **2017.**

[11] A.K. S., M. A. Srivastava, "*Credit Card Fraud Detection Using Hidden Markov Model*", IEEE, Vol. **5**, No. **1**, **2008.**

[12] T.P. Bhatla, V.Prabhu and A.Dua,. "*Understanding credit card frauds*", Cards Business Review, Tata Consultancy Services, **2003**.

[13] L. Qibei and J. Chunhua, "*Research on Credit Card Fraud Detection Model Based on Class Weighted Support Vector Machine*", Journal of Convergence Information Technology, Vol.**6,** Issue **1,** pp.**62-68, 2011.**

[14] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga and N. Kuruwitaarachchi, "*Real-time Credit Card Fraud Detection Using Machine Learning*", 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, **India**, pp. **488-493**, **2019**.

[15] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "*Credit Card Fraud Detection - Machine Learning methods*", 18th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, **Bosnia and Herzegovina**, pp. **1-5, 2019.**

[16] S. Mittal and S. Tyagi, "*Performance Evaluation of Machine Learning Algorithms for Credit Card Fraud Detection*", 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, **India**, pp. **320-324, 2019**.

[17] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "*Random forest for credit card fraud detection*", IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), **Zhuhai**, pp. **1-6, 2018.**

[18] A.Benchaji, S. Douzi and B. ElOuahidi, "*Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection*", 2nd Cyber Security in Networking Conference (CSNet), **Paris**, pp. **1-5, 2018.**

[19] R. R. Popat and J. Chaudhary, "*A Survey on Credit Card Fraud Detection Using Machine Learning*", 2nd International Conference on Trends in Electronics and Informatics (ICOEI), **Tirunelveli**, pp. **1120-1125, 2018.**

[20] J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, "*Credit card fraud detection using machine learning techniques: A comparative analysis*", International Conference on Computing Networking and Informatics (ICCNI), **Lagos**, pp. **1-9, 2017.**

[21] K. T. Hafiz, S. Aghili and P. Zavarsky, "*The use of predictive analytics technology to detect credit card fraud in Canada*", 11th Iberian Conference on Information Systems and Technologies (CISTI), **Las Palmas**, pp. **1-6, 2016.**

[22] V. Mareeswari and G. Gunasekaran, "*Prevention of credit card fraud detection based on HSVM*", International Conference on Information Communication and Embedded Systems (ICICES), **Chennai**, pp. **1-4, 2016.**

[23] A.Agrawal, S. Kumar, and A. K. Mishra, "*Implementation of Novel Approach for Credit Card Fraud Detection*", 2nd International Conference on Computing for Sustainable Global Development (INDIACom), **New Delhi**, pp. **1-4, 2015.**

Authors Profile

Mr. Kapil Dev Tripathi received Bachelor of Engineering (B.E.) from TITS, RGPV, Bhopal. I'm currently pursuing M. Tech (Master of Technoogy) in Department of CSE from ShriRam College of Engineering & Management, Gwalior, India. My area of interest Data Mining, Machine Learning and Deep Learning.

Mr. Vikash Singh Rajput received B.E. (2014) and M.tech (2017) degree from Institute of Information Technology and Management, Gwalior, Madhya Pradesh, India. He is currently working as Assistant Professor in CSE/IT Department in SRCEM, RGPV, Bhopal. He has published more than 5 Research papers in Reputed International Journals and a Conference including IEEE and it's also available online. His main research work focuses on Data Mining, Machine Learning and Deep Learning.

