Synopsis on

CONFLICT DETECTION AND RESOLUTION FOR ADAPTIVE CLASSIFICATION OF IMBALANCED DATA STREAMING DURING CREDIT CARD TRANSACTIONS

JULY-2020

Submitted for registration in the degree of

Doctor of Philosophy

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CHITKARA UNIVERSITY

HIMACHAL PRADESH

Submitted by

RINKU

PHDENG -20066

Under the supervision of

Dr. Neha Kishore,

Associate Professor,

Department of Computer Science and Engineering,

Chitkara University, Himachal Pradesh

ABSTRACT

The number of clients for the credit cards (CC) has grown of the most recent decade. These cards have disturbed the cashless frameworks of instalments just as reduced the utilization of money acknowledge, which is named as a short term continuous loan. There are various sorts of dangers in monetary space, for example, psychological oppressor financing, tax evasion, credit card falseness and protection deceitfulness that may bring about disastrous complications for bodies, for example, banks or insurance agencies. In classification issues, the slanted circulation of classes otherwise called class imbalance is a typical test in financial fraud recognition, where uncommon information mining approaches are utilized alongside the conventional classification algorithms to handle this issue. We propose an experimental investigation of the influence of class imbalance and measuring the conflict generating in the imbalanced data. We plan to identify fakes that are unnoticeable out of sight of all transactions .On the transaction level, we intend to recognize false transactions which, as far as their quality attributes, are all around discernable from real transactions.

A river has no beginning and no end in visualization. Data streaming happens where data is generated continuously rather than in batches. Traditionally data generation done in batches. In the third phase of work simulation for data streaming of credit card transaction will be implemented with the help of appropriate software

There are various classification algorithms like random forest, logistic regression, support vector machine, artificial neural network, decision tree and naive bayes etc. In the first phase of work multiple algorithms will be implemented and compared for the classification to measure the performance. This phase will provide the suitable classification method for further phases of research.

Parameters which define the model architecture are referred to as hyperparameters and thus this process of searching for the ideal model architecture is referred to as hyperparameter tuning. In the next phase hyperparameter tuning for adaptive classification for imbalanced data is implemented so that the hyperparameters define how our model is actually structured.

Conflicts are approaching issue in the credit card transactions. The conflicts are available at many levels of the process handling. Due to the conflict transactions of credit card can be declined if the verification or validations fails. In this phase imbalanced data. The next phase of research includes the design and development of an algorithm for detection and resolution of the conflict in the imbalanced data streaming of the credit card transactions.

Overall the flow of research work will start from the finding the suitable method of classification of imbalanced data with the help of the performance comparison of various classification models. In next step hyperparameter tuning for adaptive classification for imbalanced data will be implemented. After that imbalanced data streaming of credit card transactions will be simulated through appropriate software. In the last face of work designing and development of an algorithm will be done that uses the model classification method and imbalanced data streaming to detect and resolve the conflict in the transactions of credit card.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

Abbreviation	Full Name
CC	Credit Card
CNP	Card Not Present
ATM	Automated Teller Machine
PIN	Personal Identification Number
PC	Personal Computer
FDS	Fraud Detection System
DT	Decision Tree
RT	Random Tree
RBNF	Radial Basis Function Network
BMRC	Bays Minimum Risk Classifier
RF	Random Forest
BNC	Bayesian Network Classifier
ANN	Artificial Neural Network
PGA	Peer Group Analysis
BPA	Break Point Analysis
SOM	Self-Organising Map
ICLN	Improved Competitive Learning Network
GA	Genetic Algorithm
AIS	Artificial Immune System
AI	Artificial Intelligence

LIST OF ABBREVATIONS

Abbreviation	Full Name
HMM	Hidden Markov Model
WELM	Weighted Extreme Learning Machine
CCRI	Credit Card Risk Identification
SVM	Support Vector Machine
RFC	Random Forest Classifier
PRC	Precision Recall Curve
MPV	Mean Value Person
LR	Logistic Regression
CCF	Credit Card Fraud
MLT	Machine Learning Technologies
HOBA	Homogeneity Oriented Behavioural Analysis
HHEA	Hyper-Heuristic Evolutionary Algorithm
RIBIB	Risk Induced Bayesian Inference Bagging
ML	Machine Learning
ULB	Université Libre de Bruxelles, Brussels, Belgium
SCARFF	Scalable Framework for Streaming Credit Card Fraud Detection with Spark
NB	Navie Bays
TP	True Positive
TN	True Negative

LIST OF ABBREVATIONS

Abbreviation	Full Name
FP	False Positive
FN	False Negative
OTP	One Time Password
PIN	Personal Identification Number
CVV	Card Verification Values
AVS	Address Verification System
CVS	Card Verification System

1. Introduction

With the development of digitalization, deals through the web got one of fundamental business strategies for the associations, organizations, and government offices to expand their efficiency in worldwide transactions. One of the principle explanations behind the achievement of internet business is the simple online credit card transaction. At whatever point we talk about money related exchanges, we additionally need to mull over monetary fraud. Budgetary fraud is a deliberate wrongdoing where a fraudster benefits himself/herself by denying a privilege to a casualty or by acquiring monetary profit. As credit card transaction is the most well-known technique for installment in the ongoing years, the misrepresentation exercises have expanded quickly. Technologies that have been used in order to prevent fraud are Address Verification Systems, Card Verification Method and Personal Identification Number.

1.1. History of Credit Cards

Prior to the introduction of credit cards, the main installment strategies were money, check, credit extension or a credit account. In the mid-1900s, oil organizations and other corporate monsters presented card spending by means of their own exclusive cards (Gerson *et al.*, 2016) . The exclusive cards were classified "credit-cards" and they extraordinarily decreased administrative bookkeeping blunders and expanded client spending (Olaechea, 2014) . The goal behind giving these cards was to give accommodation to their clients as well as to energize client dependability. Around the 1940s, money related go between entered the credit-card industry. Their administrations included dealing with the bookkeeping and bill gathering for business and client exchanges. These go between would then work with different vendors around town which expanded clients' possibilities for shopping. Toward the day's end, organizations would turn in their business slips to the bank, including the "credit" transactions, and afterward the bank would gather the cash from the client toward the month's end. In 1946, the main bank card was presented. As indicated by MasterCard (2017), a New York broker by the name of John Biggins chose to give a card that when utilized by qualified clients at taking part organizations, the bank would repay the vendor and would then gather the cash from the client toward the month's end. Qualified clients were clients who were at Biggins' bank. In the event that a client didn't save money with Biggins, at that point they couldn't utilize this administration. The Diners Club, the principal eating/travel credit card, was created during the 1950s by Frank McNamara. While going out to eat with his significant other, he understood he

left his wallet in another suit. His significant other took care of the bill yet McNamara was so humiliated by this that he went to the proprietor of the eatery and got some information about tolerating a multi-reason credit card as installment. The proprietor was available to the thought and McNamara called different speculators to back and build up the Diners Club card in its first year, the Diners Club had more than 20,000 individuals and in its subsequent year, its part base developed to more than 42,000. Obviously, charging merchandise and enterprises turned out to be progressively well known and now it is the favored strategy for installment by most purchasers around the globe.

1.2. Credit Card Processing

There are four primary players associated with credit card handling. The first is the giving bank. The giving bank (in the future alluded to as the backer) is answerable for stretching out the credit extension to the client. Normally, backers are banks themselves and they decide a client's credit extension, loan cost and last endorsement for products and enterprises bought with the card.

The subsequent player is the processor. The processor gives a system to the client's Visa data to be transmitted from the trader to the guarantor. The processor can be thought of as the go between during the 1940s. The four significant processors in the United States are Visa, MasterCard, American Express and Discover.

The third player is the guarantor's misrepresentation security group. This administration is customarily performed by an outsider. Without a doubt, the calculations are intricate and are unquestionably safely secured. The main individuals aware of such safety efforts are officials. Infrequently, if at any time, are any delegates at the giving bank mindful of which standard is utilized while deciding if a transaction is fake.

The fourth player is the procuring bank. The procuring bank (in the future alluded to as the acquirer) is the dealer's bank and they are liable for sending the client's installment data to the processor. When the exchange gets endorsement from the processor, the client is permitted to leave with the products or have the administrations rendered. Credit card handling experiences six phases. The first is the point at which a client buys products or administrations and pays with a credit card. The second is the point at which the dealer runs the credit card. The client's data is transmitted by means of the vendor's terminal to the acquirer's system. The acquirer advances this data to the processor. The processor's system at that point speaks with the guarantor's misrepresentation recognition organization and trusts that the exchange will breeze

through the fraud assessment. When the exchange is considered non-fake, it is sent on to the backer for conclusive endorsement. At the point when this endorsement is sent, the client leaves with the merchandise or gets the administrations gave by the shipper. The backer at that point sends a bill to the client.

1.3. Types of Credit Card Transactions

Credit Card transactions fall under two classifications. The first is card present. All transactions made by swiping or embedding are a card fall under this sort. Because of the ongoing chip security highlight, on the off chance that a vendor doesn't swipe a card with the chip include, at that point the trader is exclusively dependable if that exchange is deceitful. On the off chance that they utilized the chip security include, at that point the guarantor is capable.

The subsequent kind is known as card not present. All web based business transactions fall under this class and they are the most vulnerable to credit card fraud. In the event that a deceitful transaction is card not present, at that point the shipper retains the expenses. The purpose behind this is on the grounds that the shipper can't play out the important safety efforts as well as could be expected. Since they can't use the security strategies issues by the processor or the guarantor, the dealer expect all obligation.

1.4 Types of Credit Card Fraud

Credit card fraud can be sufficiently classified into two gatherings, to be specific standard and trader. In the two kinds, fraudsters caught touchy credit card data having a place with cardholders. What separates them is the means by which cardholders' data was blocked. The principal type is the most self-evident a normal individual some way or some way or another got cardholders' data. They are a solitary element and are not running a venture or some likeness thereof. These individuals will in general be servers in cafés, programmers or trash jumpers. The other sort of fraud is acquiesced by the traders themselves. Shippers will take the cardholder's data and adventure it for their potential benefit.

1.4.1 Card not Present

If a card isn't truly present when a customer makes a purchase, the shipper must rely upon the cardholder, or someone showing to be in this way, presenting card information in an indirect way, whether or not by means of mail, telephone or over the Internet.

1.4.2 Identity Theft

This identity theft is divided into two categories

- **Application Fraud**

Application misrepresentation happens when a man uses taken or fake documents to open a record in another person's name. Guilty parties may take records, for instance, administration bills and bank clarifications to create accommodating individual information

- **Account Takeover**

This theft happens when an illegal poses as an intelligent customer, gains control of an account and then makes unofficial transactions

1.4.3 Skimming

ATM skimming is a procedure when hoodlums place a gadget on the essence of an ATM, which resembles a piece of the machine as shown in Fig-1. It is practically unthinkable for individuals to distinguish the distinction except if they are sharp security onlookers, or the skimmer is of low quality.

The lawbreakers regularly shroud a little pinhole camera in a handout holder close to the ATM. It is generally done to remove the focused on casualty's PIN. The camera is avoided the view in this way, when an obscure casualty utilizes their card to make an exchange, the card subtleties, including the pin code number, are caught. The gas siphon tricks are similarly defenseless against this sort of fraud.

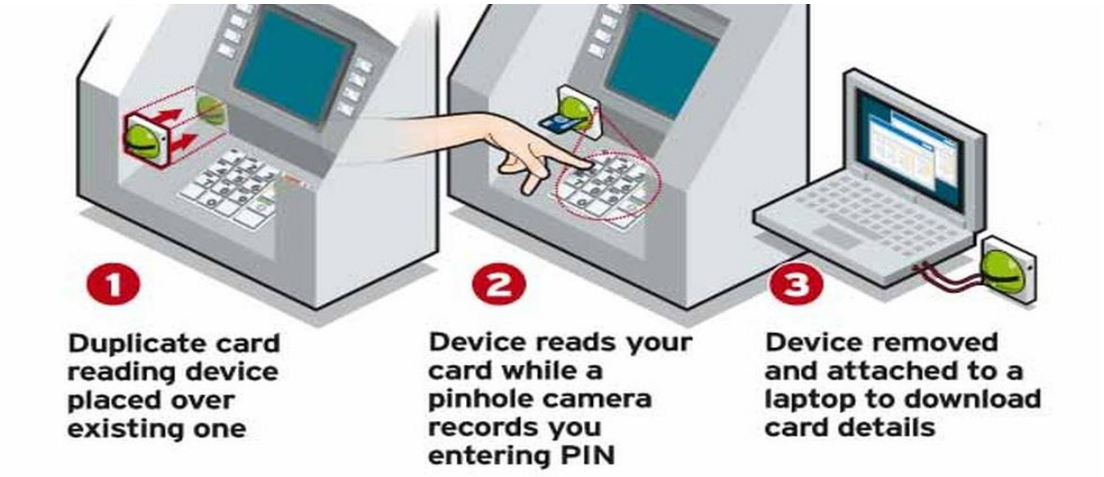

Fig-1: ATM card Skimming

Source: https://vajiramias.com/current-affairs/atm-card-skimming/5cde79c71d5def11fddf8e1b/

An electronic methodology for getting a setback's up close and personal information used by character hoodlums. The skimmer is a little contraption that yields a Visa and stores the information contained in the alluring strip. Skimming can happen in the midst of a good 'ol fashioned trade at a business.

1.4.4 Phishing

Phishing email messages, destinations, and calls are expected to take money. Cybercriminals can do this by presenting poisonous programming on your PC or removing singular information from your PC. Phishing is such a social structuring attack normally used to take customer data, including login affirmations and Master card numbers.

Fig-2: Phishing

Source: https://www.duocircle.com/content/protection-from-phishing

1.4.5 Lost and stolen card fraud

The physical security of credit cards is an important factor. If a card is not adequately protected, then it can get accidentally lost and fall in the hands of perpetrators. In some cases,

an unattended card may be stolen with ill intention. These frauds can be used to launch other frauds.

1.4.6 Counterfeit cards

Such fakes are submitted through skimming genuine credit card data and making a produced attractive tape having data about credit card.

1.4.7 Mail non-receipt fraud

This misrepresentation is otherwise called "never got issue" or "capture fraud." It happens when a client is anticipating another card or a substitution; however a criminal gets its ownership before the real client and starts utilizing it.

1.4.8 Fake cards

Credit cards might be cloned by duplicating all the data encoded in the attractive strip and gluing into another strip to get a phony card. Formation of phony cards should be possible by somebody who is sufficiently talented to manufacture the attractive strip and the chip and break the mind boggling security and even multi-dimensional images of genuine credit cards

1.4.9 Credit card imprints

Credit card engraves are taken as a proportion of the security store for administration uses like lodgings or vehicle rentals. An untrustworthy specialist organization or its worker may skim the data, which can be utilized in false exchanges.

1.4.10 Card –ID Theft

It is the most difficult misrepresentation to identify where the subtleties of credit card become known to a lawbreaker, and this data is utilized to assume control over a card record or open another one. Data fraud establishes 71% of the most widely recognized kind of fraud.

1.4.11 Clean fraud

To submit this class of fakes, the fraudster does a ton of schoolwork in gathering the client's genuine subtleties and working standards of fundamental Fraud Detection System. The framework doesn't presume such an exchange and along these lines the misrepresentation happens in a perfect way.

1.4.12 Friendly fraud

These cheats are about renouncement. Without legitimate online verification systems, the real clients may deny making a buy subsequent to doing it. The client asserts that the card has been taken before the said exchange.

1.4.13 Triangle fraud

As the name proposes, this fraud happens in three recursive advances. The first step is to make a phony internet business store or site that offers mainstream things at an exceptionally low cost. Clients are enticed to make buys at these locales and their credit cards subtleties are taken. In the subsequent advance, products are bought from different traders utilizing recently taken cards and conveyed to the buyer. The third step is to utilize the taken data to make buys somewhere else. This indirection can enable the assault to stay covered up for quite a while

1.5 Fraud Detection System (FDS)

Fraud is as old as humanity itself and can take an unlimited variety of different forms. Moreover, the development of new technologies provides additional ways in which criminals may commit fraud. Fraud detection is, given a set of credit card transactions, the process of identifying if a new authorized transaction belongs to the class of fraudulent or genuine transactions

1.6 Techniques of Fraud Detection System

Currently, the techniques used for credit card fraud detection can be classified into the following categories:

Fraud Analysis: Deals with supervised learning for identifying misuse detection

User Behavior Analysis: Deals with unsupervised learning for anomaly detection

1.6.1 Based on Supervised Learning

Supervised learning algorithms try to model relationships and dependencies between the target prediction output and the input features such that we can predict the output values for new data based on those relationships which it learned from the previous data sets. Few techniques which researchers (Dal Pozzolo *et al.*, 2018) (Patil, Nemade and Soni, 2018) (Lucas *et al.*, 2020)(Mandal *et al.*, 2016) have used in credit card fraud detection are:

- Discriminant Analysis
- Decision Trees and Random Trees
- Radial Basis Function Networks
- Meta-Classifier
- Bays Minimum Risk Classifier
- Random Forest
- Bayesian Network Classifier
- Artificial Neural Network
- Deep Learning
- Decision Tree Based Classifier
- Hybrid Supervised Approach

1.6.2 Based on Un-Supervised Learning

Un-supervised learning is valuable in contemplates that need to distinguish changes in conduct or bizarre exchanges. Real named deceitful and ordinary exchanges are not accessible. An underlying arrangement of exchanges considered as would be expected is utilized to begin the classification procedure. Few unsupervised learning discussed by various researchers (Mittal and Tyagi, 2019)(Kumar, 2018)(Fiore *et al.*, 2019):

- Peer Group Analysis
- Break Point Analysis
- Self-Organizing Map
- Improved Competitive Learning Network
- Adversarial Learning

1.6.3 Based on Nature inspired

- Genetic Algorithm
- Artificial Immune System

2. Literature Review

Credit card fraud is perhaps the most serious peril to business establishments today. Regardless, to fight the deception feasibly, it is basic to initially understand the frameworks of executing a cheat. Credit card fraudsters use an incalculable regular strategy to submit blackmail. In essential terms, Credit card fraud is described as "exactly when an individual uses another individuals' cards information for singular reasons while the owner of the card and the card patron don't think about how the card is being used" (Kim *et al.*, 2019). Further, the individual using the card has no relationship with the cardholder or sponsor and has no point of either arriving at the owner of the card or making repayments for the purchases distracted.

Credit card frauds are given in the accompanying manners:

- A show of criminal precariousness (mislead with desire) by use of unapproved account or conceivably singular information.
- Unlawful or unapproved usage of records for singular get.
- Deception of record information to get items and moreover benefits.

Table-1: Literature review

Pub-Year	**Authors**	**Title**	**Source**	**Indexing**	**Summary**
2020	Elena-Adriana Minastireanu, Gabriela Mesnita	Methods of Handling Unbalanced Datasets in Credit Card Fraud Detection (Minastirean *et al.*, 2020)	Broad Research in Artificial Intelligence and Neuroscience	Emerging Sources Citation Index	In this paper, authors discussed about the various techniques to handle the unbalanced data. The authors precisely implement the classification techniques to find the sensitivity, specificity, precision, recall and accuracy in the unbalanced dataset in credit card fraud detection.
2020	Yvan Lucas , Pierre-Edouard Portier, Léa Laporte,	Towards automated feature engineering for credit	Future Generation Computer Systems	Science Citation Index Expanded	In this research work, authors proposed an HMM-based element designing technique that permits them to join successive information in the exchanges as

	Liyun He-Guelton, Olivier Caelen, Michael Granitzer, Sylvie Calabretto	card fraud detection using multi-perspective HMMs (Lucas *et al.*, 2020)			HMM-based highlights. These HMM-based highlights empower a non-consecutive classifier (Random Forest) to utilize successive data for the grouping
2020	Gabriele Gianini, Leopold Ghemmogne Fossi, Corrado Mio, Olivier Caelen, Lionel Brunie, Ernesto Damiani	Managing a pool of rules for credit card fraud detection by a Game Theory based approach (Gianini *et al.*, 2020)	Future Generation Computer Systems	Science Citation Index Expanded	In this paper the author addressed the following points: the criteria used to select which rules to keep operational in the NRT pool are traditionally based on the historical performance of the individual rules, considered in isolation. This approach disregards the non additivity of rule composition within the pool. Authors proposed to use an approach based on estimating the individual rule contribution to the overall pool performance through the Shapley Value (SV).
2020	Inaki Aldasoro, Leonardo Gambacorta, Paolo Giudici and Thomas Leach	The drivers of cyber risk (Aldasoro, *et al.*, 2020)	BIS Working Papers , SSRN Press	Elsevier, Scopus	In this paper authors discussed about few conflicts of interest in the banking domain. The authors highlighted the conflicts in the financial transactions required to be address.
2020	Honghao Zhu, Guanjun Liu, Mengchu	Optimizing Weighted Extreme	Neurocomputing	Science Citation Index	In this paper, author uses three improved dandelion algorithms with probability-based mutation to

	Zhou, Yu Xie, Abdullah Abusorrah, Qi Kang	Learning Machines for Imbalanced Classification and Application to Credit Card Fraud Detection (Zhu *et al.*, 2020)		Expanded	optimize the parameters of WELM, and propose three optimized WELMs for imbalanced classification problems. Experimental results show that the three optimized WELMs can achieve better classification performance than the compared algorithms on 14 imbalanced datasets. This work also applies the proposed WELMs to credit card fraud detection, and the results show their effectiveness.
2020	Naoufal Rtayli, Nourddine Enneya	Selection Features and Support Vector Machine for Credit Card Risk Identification (Rtayli *et al.*, 2020)	13th International Conference Interdisciplinary in Engineering	Science Citation Index Expanded	The proposed algorithm included a few enhancements regarding CCRI that help to increment both the affectability and the grouping execution, which are the most significant measures to assess the Credit Card Risk Identification model. The primary focal points of SVM dependent on RFC are: Firstly, the model has a decent precision rate to 95%. Furthermore, it diminishes the quantity of bogus positive exchanges by improving the affectability rate to 87% in a huge and lopsided dataset where the pace of fraud is low (<0.17%), which is exceptionally advantageous for the organizations to limit the high credit of examination movement. At last, it

					has a high rate (91%) in term of grouping execution
2020	Admel Husejinović	Credit card fraud detection using naive Bayesian and C4.5 decision tree classifiers (Husejinović, 2020)	Periodicals of Engineering and Natural Sciences	Scopus	Generally discussed as indicated by the PRC Area by and large best performing calculation is packing with a C4.5 choice tree as a base student with a pace of 1,000 for class 0 and 0,825 for class 1. Most elevated review paces of 0,978 for class 0 and 0,829 for class 1 are recorder in the exhibition of the Naive Bayes model. Most elevated accuracy paces of 1,000 for class 0 and 0,927 for class 1 are recorder in the exhibition of the C4.5 choice tree model. In the event that it remain that the dataset is very imbalanced PRC paces of 1,000 for class 0 and 0,825 for the class are very encouraging
2020	Younus Ahmad Shah, Sorab Kumar	Detecting frauds from credit card transaction using improved approach of random forest learning and MPV classification (Shah,	Studies in Indian Place Names	UGC care List	In this paper a mechanized framework that uses MPV alongside the Random Forest learning calculation for recognizing fraud proposed. The pre-preparing stage is basic and is all around characterized utilizing clamor taking care of and resizing activity. The got dataset is taken care of into the prepared system for include Confusion Matrix extraction utilizing the Random Forest learning calculation and arrangement is performed utilizing

		Kumar *et al.*, 2020)			MPV. The half and half methodology followed give better outcomes. The fundamental goal of the proposed writing is to make enhanced recognition utilizing Random Forest for better precision. Higher exactness is accomplished by the utilization of said writing. Later on, the proposed methodology can be inspected against the constant datasets for better assessment of the exactness
2019	Niloofar Yousefi, Marie Alaghband, Ivan Garibay	A Comprehensive Survey on Machine Learning Techniques and User Authentication Approaches for Credit Card Fraud Detection (Yousefi, *et al.*, 2019)	Machine Learning	Scopus	In this review, authors saw that administered learning strategies have been utilized more much of the time than solo techniques. To be more specific, the most normally utilized fraud detection techniques are LR, ANN, DT, SVM, and NB.
2019	Vaishnavi Nath Dornadula, Geetha S	Credit Card Fraud Detection using Machine	International Conference on Recent Trends in Advanced	Science Citation Index	In this paper the author developed a novel method for fraud detection, where customers are grouped based on their transactions and extract behavioral

		Learning Algorithms (Dornadula *et al.*, 2019a)	Computing		patterns to develop a profile for every cardholder. Then different classifiers are applied on three different groups later rating scores are generated for every type of classifier. These dynamic changes in parameters lead the system to adapt to new cardholder's transaction behaviors timely. Followed by a feedback mechanism to solve the problem of concept drift.
2019	Ajeet Singh and Anurag Jain	Adaptive Credit Card Fraud Detection Techniques Based on Feature Selection Method (Jain, 2019)	Advances in Computer Communication and Computational Sciences	Scopus	In this investigation, Credit card fraud (CCF) has been classified into two classifications application-level cheats, and exchange level fakes. The German dataset has been utilized to distinguish application-level fakes through Machine Learning Technologies (MLTs) with the assistance of highlight determination techniques. The utilization of MLTs is benefited from filter and covering strategies for choosing extremely high associated highlights that are compelling for diminishing the runtime, off base forecast, and expanding the expectation precision of classifiers.
2019	Alex Sangers, Maran van Heesch,	Secure Multiparty PageRank	International Conference on Financial	Springer, Scopus	Existing procedures for fraud detection would exceptionally benefit from a coordinated effort

	Thomas Attema, Thijs Veugen, Mark Wiggerman, Jan Veldsink, Oscar Bloemen, and Dani¨el Worm	Algorithm for Collaborative Fraud Detection (Sangers *et al*, 2019)	Cryptography and Data Security		between financial organizations. In any case, the trading of important data is frequently constrained, or not even conceivable, because of protection limitations or business confidentiality. This paper showed that protected multiparty calculations can help tackle this test.
2019	Eunji Kim , Jehyuk Lee, Seung-kwan Nam ,Hunsik Shin , Youngmi Song , Hoseong Yang , Jeong-a Yoon , Sungzoon Cho , Jong-il Kim	Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning (Kim *et al.*, 2019)	Expert Systems With Applications	Science Citation Index Expanded	In the credit card business, it was a setup standard to build up the fraud detection system as a troupe of various models. The authors led a top to the bottom relative investigation between profound learning and cross breed troupe with different commonsense assessment measurements to figure out which models perform better than the other on enormous true exchange information. The champion challenger structure is acquainted in this paper with creating and analyze the two models
2019	Xinwei Zhang, Yaoci Han, Wei Xu, Qili Wang	HOBA: A novel feature engineering methodology for credit card fraud detection with a deep	Information Sciences	Science Citation Index Expanded	This paper proposes a novel feature engineering framework with a deep learning architecture for credit card fraud detection. A feature engineering framework based on a homogeneity-oriented behavior analysis (HOBA) is proposed to generate the feature variables representing the behavior

		learning architecture (Zhang *et al.*, 2019)			information for fraud detection models. Compared to previous works, author's feature engineering framework takes the heterogeneity of credit card transactions into consideration and carries out a behavior analysis only on homogenous transactions.
2019	Fabrizio Carcillo Frederic Oble, Yann-Ael Le Borgne , Gianluca Bontempi ,Olivier Caelen , Yacine Kessac	Combining unsupervised and supervised learning in credit card fraud detection (Carcillo *et al.*, 2019)	Information Sciences	Science Citation Index Expanded	This paper proposes the execution of a hybrid methodology that utilizes solo anomaly scores to broaden the list of capabilities of a misrepresentation discovery classifier. The curiosity of the commitment, past its applications in genuine and sizeable datasets of credit card transactions, is the usage and evaluation of various degrees of granularity for the definition of an exception score. The granularity being referred to ranges from the card level to the worldwide level, thinking about the middle of the road levels of card total through grouping
2019	Younus Ahmad Shah, Er Sorab Kumar	Online transaction fraud detection mechanisms : a comparative analysis (Younus *et*	Journal of the Gujarat Research Society	UGC care List, Open access	In this paper authors discussed about the methods used to identify fraud inside the online transactions. This perspective is basic since the cutting edge period is moving towards cashless transactions. This viewpoint in spite of the fact that it is improving so does the danger of fraud by

		al., 2019)			malicious clients. This paper gives the subtleties of methods used to distinguish such frauds alongside a bit of flexibility and problem of each. The authors inferred that missing information taking care of alongside constrained uses of detection system causes higher mistake rate and low characterization exactness.
2019	Ugo Fiore, Alfredo De Santis, Francesca Perla, Paolo Zanetti, Francesco Palmieri	Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection (Fiore *et al.*, 2019)	Information Sciences	Science Citation Index Expanded	In this work, a system is introduced to manage the issue of class lopsidedness in the utilization of administered classification to the recognition of credit card misrepresentation. Given a preparation set, an enlarged set is created, containing more instances of the minority class as for the first.
2019	Deshen Wang , Bintong Chen, Jing Chen	Credit card fraud detection strategies with consumer incentives (Wang, *et al.*, 2019)	Omega	Science Citation Index Expanded	In this paper, the author talks about a system for a shipper to forestall deceitful credit card transactions. They first look at two systems that are utilized by and by no counteraction (Strategy 1) and utilizing the ML identification model for all exchanges (Strategy 2). They likewise examine Strategy 3, in which optional

					verification is mentioned for all exchanges, with a motivating force for shoppers. Authors find that three boundaries (fraud rate, customers' pace of surrendering authentic transactions that are erroneously declined by an ML identification model, and the motivator required to repay the shopper for the burden of auxiliary verification) can catch the issues engaged with fake credit card transactions.
2018	Alex G.C. de Sa , Adriano C.M. Pereira, Gisele L. Pappa	A customized classification algorithm for credit card fraud detection (de Sa, *et al.*, 2018)	Engineering Applications of Artificial Intelligence	Science Citation Index Expanded	This work presented Fraud-BNC, a customized Bayesian Network Classifier (BNC) algorithm to solve a real-world credit card fraud detection problem. The Fraud-BNC algorithm was automatically generated by a Hyper-Heuristic Evolutionary Algorithm (HHEA), which creates customized solutions for classification datasets. Fraud-BNC was evaluated on a dataset from PagSeguro. Nevertheless, this algorithm is general enough to solve other classification problems from the literature.
2018	Akila S, Srinivasulu Reddy U	Cost-sensitive Risk Induced Bayesian	Journal of Computational Science	Science Citation Index Expanded	Misrepresentation discovery in credit card transactions are an issue requiring arrangements adjusted to the business objectives of associations, specifically

		Inference Bagging (RIBIB) for credit card fraud detection (Akila *et al.*, 2018)			regarding cost. In any case, not very many examination commitments approach the issue from this point of view. This paper proposes a cost-sensitive fraud detection model for credit card transactions that adjusts adequately with the business objectives of associations by giving practical forecasts. The proposed RIBIB design is a troupe based model joining three commitments in the area of stowing groups. The RIBIB model proposes a compelled sack creation approach that has been specifically intended for taking care of imbalanced information, a hazard incited likelihood-based base student model for diminishing the expected cost and a cost-touchy weighted democratic combiner for second-level cost decrease. The RIBIB model was seen to display low computational necessities because of the utilization of a probabilistic indicator and a successive workflow. Despite the fact that the proposed RIBIB model doesn't acclimate with ordinary measurements, it intends to give immense benefits regarding cost.
2018	Nick F.	How	Engineering	Science	Fraud Losses have developed each

	Ryman-Tubb, Paul Krause, Wolfgang Garn	Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark (Ryman-Tubb *et al.*, 2018)	Applications of Artificial Intelligence	Citation Index Expanded	year since 1971 regardless of the safeguard furthermore, location strategies set up. These techniques have not been adequately effective either in the group of work studied or in conveyed arrangements. There are two clarifications for the disappointment of these techniques, (1) That there is little industry motivating force to improve them while fraud levels are decided as an expense of business and are viewed as regularizing. (2) Scholarly work around there is troublesome furthermore, minimized regarding subsidizing.
2018	Sanaz Nami , Mehdi Shajari	Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors (Nami *et al.*, 2018)	Expert Systems With Applications	Science Citation Index Expanded	Payment card fraud is an enormous issue for the Banking area. Henceforth, a successful fraud location framework for card installments is required by any bank or money related organization to lessen the harms brought about by fake exercises. In this paper, the author expected that deviation from the typical conduct of the cardholder could fill in as the reason for fraud identification
2018	Suraj Patil,Varsha Nemade, PiyushKumar	Predictive Modeling For Credit Card Fraud	International Conference on Computation	Science Citation Index Expanded	In this paper, the authors have proposed a robust framework to process an enormous volume of information, the usefulness of the

	Soni	Detection Using Data Analytics (Patil, *et al.*, 2018)	al Intelligence and Data Science		system can be reached out to separate continuous information from various unique sources. The extricated information is then used to assemble a solid investigative model. To improve the expository exactness of fraud forecast, creators have executed three distinctive scientific strategies. These detection models are run on credit card datasets and the precision of the explanatory model is assessed with the assistance of the disarray grid.
2018	Johannes Jurgovsky, Michael Granitzer, Konstantin Ziegler, Sylvie Calabretto, Pierre-Edouard Portier, Liyun He-Guelton, Olivier Caelen	Sequence Classification for Credit-Card Fraud Detection (Jurgovsky *et al.*, 2018)	Expert Systems With Applications	Science Citation Index Expanded	In this paper, the author employed long short-term memory networks as a means to aggregate the historic purchase behavior of credit-card holders with the goal to improve fraud detection accuracy on new incoming transactions. The author compared the results to a baseline classifier that is agnostic to the past. The author showed that offline and online transactions exhibit very different qualities with respect to the sequential character of successive transactions
2018	Rafiq Ahmed Mohammed, Kok-Wai Wong, Mohd Fairuz	Scalable Machine Learning Techniques for Highly	Pacific Rim International Conference on Artificial Intelligence	Scopus, Springer	Ongoing credit card fraud location is a difficult issue due to profoundly imbalanced enormous information. This research paper depends on tests that thought about

	Shiratuddin, Xuequn Wang	Imbalanced Credit Card Fraud Detection: A Comparative Study (Mohammed *et. al* , 2018)			a few mainstream ML methods and researched their appropriateness as an "adaptable calculation" when working with exceptionally imbalanced huge or "Big" datasets.
2018	Navanshu Khare and Saad Yunus Sait	Credit Card Fraud Detection Using Machine Learning Models and Collating Machine Learning Models (Khare *et al.*, 2018)	International Journal of Pure and Applied Mathematics	SCOPUS indexed	From the trials, the outcome that has been finished up is that Logistic relapse has an exactness of 97.7% while SVM shows the precision of 97.5% and the Decision tree shows the precision of 95.5% however the best outcomes are gotten by Random woodland with exact exactness of 98.6%. The outcomes got in this manner reason that Random woodland shows the most exact and high exactness of 98.6% in the issue of credit card fraud identification with dataset gave by ULB machine learning group.
2018	Fabrizio Carcillo, Andrea Dal Pozzolo, Yann-Ael Le Borgne,Olivier Caelen, Yannis	SCARFF: a Scalable Framework for Streaming Credit Card Fraud Detection	Information Fusion	Science Citation Index Expanded	The paper introduced SCARFF, a unique adaptable stage to consequently recognize cheats in a close to the continuous skyline. The most unique commitment of this system is the plan and the execution of an open-source large information answer for certifiable

	Mazzer, Gianluca Bontempi	with Spark (Carcillo *et al.*, 2018)			Fraud Detection and its test on an enormous certifiable informational index.
2017	Professor. Vikrant Agaskar, Megha Babariya, Shruthi Chandran, Namrata Giri	Unsupervised Learning for Credit Card fraud detection (Vikrant Agaskar *et al.*, 2017)	International Research Journal of Engineering and Technology	UGC Care List	This paper has proposed another way to deal with transactions observing and credit card fraud location utilizing unaided learning. It empowers the computerized production of exchange checking rules in a learning procedure and makes conceivable their ceaseless improvement in a domain of powerfully changing data in a mechanized framework.
2016	Aisha Abdallah, Mohd Aizaini Maarof, Anazida Zainal	Fraud detection system: A survey (Abdallah, *et al.*, 2016)	Journal of Network and Computer Applications	Science Citation Index Expanded	Fraud cases have expanded lately, especially in significant and touchy specialized zones. Thus, there is a critical need to battle fraud. Fraud anticipation and discovery is the correct security instrument against fraud. Fraud anticipation alone isn't sufficient. Fraud recognition is proposed to secure imperative administrations in the specialized frameworks. This study article has investigated the best in class fraud recognition frameworks in five regions of frauds. The most normally utilized fraud recognition method is artificial neural networks (ANN), Support vector machines (SVM), rule-acceptance procedures, decision trees, strategic relapse,

					and meta-heuristics, for example, hereditary calculations.
2014	Djeffal Abdel hamid , Soltani Khaoula, Ouassaf Atika	Automatic Bank Fraud Detection Using Support Vector Machines (Abdelhamid *et al.*, 2014)	Proceedings of the International conference on Computing Technology and Information Management	Open Access	The battle against fraud is a current requirement for different areas and banks specifically. It is in this setting the authors propose a framework for identifying bank fraud dependent on help vector machines procedure, contingent upon the application in the bank. Authors concentrated in this specific circumstance, three instances of fraud in banks: credit card fraud illegal tax avoidance and home loan fraud. The authors proposed, in this setting a technique dependent on the hybridization of single class and double SVM strategies

2.1.Tools and Technologies

Various tools and technologies are using in a credit card fraud detection system.

- Amazon Storm for data streaming analytics
- Sandbox for simulation of credit cards transactions
- Python for Machine Learning
- Jupytor for Running Python
- Card Verification Values
- Address Verification System
- Card Verification System

3. Justification of Research

The research is to be proposed that will focuses on current and futures trends in credit card fraud detections systems. Financial organizations such as banks, insurance and loan companies are found at very high risk of frauds as per the previous studies.

In 2014 authors(Abdel *et al.*, 2014) proposed an automatic bank fraud detection system using support vector machine, was capable of finding the credit card frauds, illegal tax avoidance and home loan fraud in some circumstances. The authors propose, in this system a technique dependent on the hybridization of single class and double SVM strategies. In 2016 authors(Abdallah, *et al.*, 2016) discussed the higher rate of fraud in different organizations and individual level. The authors represent a survey of a fraud detection system.

In 2017 authors (Vikrant Agaskar *et al.*, 2017) suggested the fraud detection system based on unsupervised learning mechanism. A group of authors (Carcillo *et al.*, 2018) designed a system SCARFF based on the spark that is able to detect the frauds its test on an enormous certifiable informational index. Authors also implemented the fraud detection system using machine learning algorithms and find the accuracy better level from previous system. Few authors (Jurgovsky *et al.*, 2018) conducted the comparative study of the previous fraud detection system using imbalanced data. Another group of author tried to sequence classification for credit card fraud detection.

Authors (Fiore *et al.*, 2019) suggested a generative approach to improving the classification effectiveness in credit card fraud detection. Few authors (Shah, Kumar and Scholar, 2019) tried detecting frauds from credit card transaction using improved approach of random forest learning and MPV classification. A group of authors (Yousefi, Alaghband and Garibay, 2019) have done comprehensive survey on machine learning techniques and user authentication approaches for credit card fraud detection. Adaptive credit card fraud detection techniques based on feature selection method secure multiparty pagerank algorithm for collaborative fraud detection. Authors (Kim *et al.*, 2019) also implemented credit card fraud detection hybrid ensemble and deep learning algorithms. A researcher group (Zhang *et al.*, 2019) proposed a model HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture . In paper authors (Mînăstireanu and Meșniță, 2020) proposes methods of handling unbalanced datasets in credit card fraud detection. Another side authors (Lucas *et al.*, 2020)implemented a HMM model towards automated feature engineering for credit card fraud detection using multi-perspective. An author's group (Zhu *et al.*, 2020)

studies the machine learning for imbalanced classification and application to credit card fraud detection . Authors (Rtayli and Enneya, 2020) identified a methodology based on selection features and support vector machine for credit card risk identification. Few of the researchers (Husejinović, 2020) implemented credit card fraud detection using naive Bayesian and c4.5 decision tree classifiers.

The above studies shows a vast demand and need to work in financial fraud detections specially in credit card fraud detection because it deals directly to the individuals and the organizations.

3.1.Motivation

Different facets are the driving factors of this research. The financial impact of fraudulent activities is mostly catastrophic. A large number of organizations and individuals are victimized by fraudsters every day. Unfortunately, this trend is increasing every year. This by extension has a socio-cultural impact. Therefore, the financial impact of fraudulent activities is the key factor that drove this research initiative. Moreover, there are several challenges remained unsolved for building efficient fraud analytics. These challenges are critical barriers that must be solved to fight against the fraudsters. This is another important factor that motivated the research. Credit card transactions are generated with a very high speed everywhere, and very few of these transaction are cheated or fraud transaction. The data of these transactions are very large. Criminal activities are also increasing as the in the usage of credit card increased. Due to the variety of cases, e.g., cyber-attacks conducted by IT (Information Technology) specialists, civil cases in a corporation, or criminal cases, different investigators tend to follow different methods in their investigative process; there is no standard workflow in digital forensic investigation. Generally in the classification problems, four types of cases can be defined. With the knowledge of the bank at a given time, these cases are defined as follows. The True Negatives (TNs) are negatives for which no alert has been generated. As mentioned above, the data is imbalanced and there are significantly more negatives than positives, and thus the chances are high that there are a lot of TNs. True Positives (TPs) are positives which have been detected by the detector. The system only has a brief moment to determine whether an incoming transaction is fraudulent, because the system cannot hinder normal transactions. In normal settings, there are only a few positives compared to the number of negatives. So there can also only be a few TPs compared to the negatives.

False Negatives (FNs) are positives which are not detected by the detector. The cost of undetected fraudulent transactions can be high for the customers. A customer may notice the fraud themselves and report this to the bank. This feedback can then be used to improve the detection. False Positives (FPs) are negatives for which an alert has been generated. In domains of detection, these are also called false alerts. It is difficult to measure the cost of one FP. Therefore it is need of hour to reduce the false positive.

3.2.Research Gaps

Building a powerful, constant, and adaptable calculation based mechanized FDS is exposed to a few difficulties and difficulties counted in Fig-3.

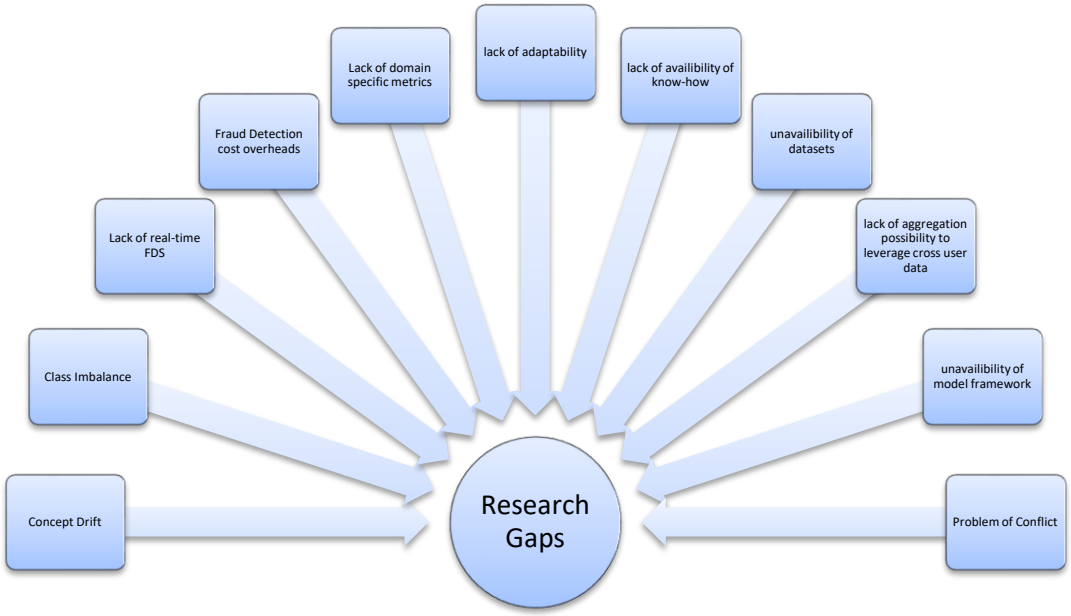

Fig-3: Research Gaps

- **Concept Drift**

FDS focusing on odd conduct experience the ill effects of the way that in reality, the profile of ordinary and deceitful conduct changes with time (Dornadula and Geetha, 2019b). For computational procedures, this prompts a non-stationary impact in displaying the connection among ward and target factors (Dal Pozzolo *et al.*, 2018).

- **Class Imbalance**

Credit card transactions data are a typical case of highly imbalanced data. In per unit of time, a large number of credit card transactions take place and most of them are genuine (Kim *et al.*, 2019). Typically, out of each 10,000 transactions, only 1 has been found to be fraudulent. Traditional computational methods perform poorly in recognizing instances of rarely occurring class, which is actually the class of interest in FDS (Dal Pozzolo *et al.*, 2018).

- **Lack of Real-Time FDS**

The vast majority of the current FDS detailed in writing chip away at recorded information that can be utilized to drive future security approaches and legal sciences (Gianini *et al.*, 2020). This investigation is compelling in a restricted way to recognize and square false exchanges continuously (Subbulakshmi, Mathew and Shalinie, 2010).

- **Fraud Detection Cost Overheads**

Many related examinations helpfully overlook the overheads in actualizing FDS (Nami and Shajari, 2018). Cost is anyway significant thought while assessing the viability of any arrangement (Dreibholz *et al.*, 2019).

- **Lack of Domain-Specific Metrics**

Existing models have been assessed based on standard classifier measurements . No standard area specific measurements are accessible to especially benchmark the exhibition of credit card FDS (Fiore *et al.*, 2019).

- **Lack of Adaptability**

Conduct examination based fraud identification strategies define typical conduct from past real exchanges of a client. Numerous a period client conducts may advance because of outside elements like family conditions, an expansion or reduction in pay, and incessant voyaging (Mittal and Tyagi, 2019). Existing administered and unaided methodologies utilized in misrepresentation location frameworks are not versatile to evolving datasets. In this manner,

the efficiency of distinguishing new examples of ordinary and false practices becomes difficult (Tariq, 2018).

- **Lack of Availability of Know-How**

Existing fraud detection systems are not made open because of the dread of them being lesser compelling (Richardson *et al.,* 2020). In this manner, everybody needs to re-concoct the haggle information can't be utilized (G and R, 2018).

- **Unavailability of Datasets**

Credit card organizations don't release their marked datasets for open examination. Numerous computational strategies depend on gaining from datasets (Misra *et al.,* 2020). Indeed, even a couple datasets that are openly accessible are really a handled type of genuine datasets to conceal genuine factors and their relations (Ryman-Tubb, Krause and Garn, 2018).

- **Lack of Aggregation Possibility to Leverage Cross User Data**

Ideally utilizing exchange information across card-giving organizations and sorts of cardholders are unrealistic because of an absence of trust among card-giving organizations (Jurgovsky *et al.*, 2018).

- **Unavailability of standard FDS framework**

There are many methods and algorithms present to detect the fraud due to credit card usage. Some authors proposed the frameworks according to their implementation of FDS (Kim *et al.*, 2019). There is no fixed framework available according to that the fraud detection system can be designed and implemented (Lucas *et al.,* 2020).

- **Problem of conflict**

Credit card transactions are generated with high rate and having conflicts in the transactions (Song, Wang and Hu, 2019). Due to the conflict many times transactions are declined by either merchant or the server processing the transactions (Jung, 2020).

4. Problem Statement

Study of the literature confines that the fraud using credit card would be increasing at a very higher rate along with the higher data volume. Organizations are using various fraud detection systems in the traditional way for their business operations. In a large volume of data, finding fraudulent transaction is still a lengthy and time consuming process. Sometime it takes number of days to months to find the fraud transaction from a huge amount of evidential data. There are multiple gaps in the previous researches in the models those were implemented. Conflicts are also available in the transactions. Researchers are still working to find the fraudulent transaction in the real-time. Proposed research focuses with the classification of imbalanced data generated from the data streaming of credit card transactions and finding and resolving the conflicts in the transactions.

4.1. Objectives

The main objectives of the proposed study are as follows:

- To simulate the data streaming of credit card transactions and generate the dataset
- To implement the existing algorithms for imbalance data streaming during credit card transactions and compare their performance for imbalanced data classification
- To implement the hyperparameter tuning in adaptive classification for imbalanced data
- To design and develop an algorithm for detection and resolution of conflicts in the imbalanced data streaming and testing the performance for imbalanced data stream

4.2. Methodology

The table given below expresses the methodology used in the implementation of the above defined objectives.

Table-2: Research Methodology

Objectives	**Activity**	**Method**
To simulate the data streaming of credit card transactions and generate the dataset	I. Study the data streaming and their mechanism for credit card transaction II. Simulate the data streaming	Study and simulate data streaming of credit card transactions.

	of credit card transaction.	
To implement the existing algorithms and compare their performance for imbalanced data classification	III. Study the various classification methods and its implementation on imbalanced data IV. Study the advantages and weakness of the different classification methods V. Comparative analysis of various classification methods.	Analyze of various pre-existing classification methods and compare the result obtained from these methods.
To implement the hyperparameter tuning in adaptive classification for imbalanced data	VI. Study the suitable classification model for hyperparameter tuning. VII. Implement the hyperparameter tuning for adaptive classification	Study and implement the hyperparameter tuning for adaptive classification for imbalanced data
To design and develop an algorithm for detection and resolution of conflicts in the imbalanced data streaming and testing the performance for imbalanced data stream	VIII. Design, develop and implement the algorithm for conflict detection and resolutions and performance analysis. IX. Thesis writing	Design and implement the algorithm to detect and resolve the conflicts in the imbalanced data streaming

5. Expected Outcomes

- Simulation of imbalanced data streaming of credit card transactions.
- Performance comparison of various imbalanced data classification algorithms
- Hyperparameter tuning for imbalanced data
- Algorithm to detect and resolution of the conflict in credit card transaction
- At-least two-three research papers in Scopus Indexed Journals

6. Work Plan

In the work plan the activities column has symbolic roman number as activities mentioned in the above Table-2.

Table-3: Timelines to achieve objectives

Objectives	Activities	Sept – Dec '19	Dec – Mar '20	Mar-Jun'20	July '20-Oct '20	Nov-Jan'21	Feb-Apr'21	May-June'21
1	**I.**							
	II.							
	III.							
2	**IV.**							
	V.							
3	**VI.**							
	VII.							
4	**VIII.**							
	IX.							

7. References

Abdallah, A. *et al.*. (2016) 'Fraud detection system: A survey', *Journal of Network and Computer Applications*, 68, pp. 90–113. doi: 10.1016/j.jnca.2016.04.007.

Abdelhamid, D. *et al.* (2014) 'Automatic Bank Fraud Detection Using Support Vector Machines', *The International Conference on …*, pp. 10–17. Available at: http://sdiwc.net/digital-library/automatic-bank-fraud-detection-using-support-vector-machines.

Akila, S. *et al.* (2018) 'Cost-sensitive Risk Induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection', *Journal of Computational Science*. Elsevier B.V., 27, pp. 247–254. doi: 10.1016/j.jocs.2018.06.009.

Aldasoro, I. *et al.* (2020) 'The drivers of cyber risk', (865) ISSN 1682-7678,SSRN PRESS

BIS Working Paper No. 865, Available at SSRN: https://ssrn.com/abstract=3613173.

Sangers *et al.* (2019) 'Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection', in *International Conference on Financial Cryptography and Data Security*.

Carcillo, F. *et al.* (2018) 'SCARFF: A scalable framework for streaming credit card fraud detection with spark', *Information Fusion*, 41, pp. 182–194. doi: 10.1016/j.inffus.2017.09.005.

Carcillo, F. *et al.* (2019) 'Combining unsupervised and supervised learning in credit card fraud detection', *Information Sciences*. Elsevier Inc., (xxxx). doi: 10.1016/j.ins.2019.05.042.

Dal Pozzolo, A. *et al.* (2018) 'Credit card fraud detection: A realistic modeling and a novel learning strategy', *IEEE Transactions on Neural Networks and Learning Systems*. IEEE, 29(8), pp. 3784–3797. doi: 10.1109/TNNLS.2017.2736643.

Dornadula, V. *et al.* (2019a) 'Credit Card Fraud Detection using Machine Learning Algorithms', *Procedia Computer Science*, 165(20), pp. 631–641. doi: 10.1016/j.procs.2020.01.057.

Dreibholz, T. *et al.* (2019) 'Mobile Edge as Part of the Multi-Cloud Ecosystem: A Performance Study', *Proceedings - 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2019*, pp. 59–66. doi: 10.1109/EMPDP.2019.8671599.

Fiore, U. *et al.* (2019) 'Using generative adversarial networks for improving classification effectiveness in credit card fraud detection', *Information Sciences*. Elsevier Inc., 479, pp. 448–455. doi: 10.1016/j.ins.2017.12.030.

G, S. and R, J. R. (2018) 'A Study on Credit Card Fraud Detection using Data Mining Techniques', *International Journal of Data Mining Techniques and Applications*, 7(1), pp. 21–24. doi:

10.20894/ijdmta.102.007.001.004.

Gerson, *et al.* (2016) *The History of Credit Cards.*, *CreditCards.com*. Available at: https://www.creditcards.com/credit-card-news/history-of-credit-cards/ (Accessed: 12 January 2020).

Gianini, G. *et al.* (2020) 'Managing a pool of rules for credit card fraud detection by a Game Theory based approach', *Future Generation Computer Systems*. Elsevier B.V., 102, pp. 549–561. doi: 10.1016/j.future.2019.08.028.

Husejinović, A. (2020) 'Credit card fraud detection using naive Bayesian and c4.5 decision tree classifiers', *Periodicals of Engineering and Natural Sciences*, 8(1), pp. 1–5. doi: 10.21533/pen.v.

Jain, A. S. and A. (2019) 'Adaptive Credit Card Fraud Detection Techniques Based on Feature Selection Method', *Advances in Computer Communication and Computational Sciences*.

Jung, H. (2020) 'The Impact of Ambient Fine Particulate Matter on Consumer Expenditures', *Sustainability*, 12(5), p. 1855. doi: 10.3390/su12051855.

Jurgovsky, J. *et al.* (2018) 'Sequence classification for credit-card fraud detection', *Expert Systems with Applications*. Elsevier Ltd, 100, pp. 234–245. doi: 10.1016/j.eswa.2018.01.037.

Kim, E. *et al.* (2019) 'Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning', *Expert Systems with Applications*. Elsevier Ltd, 128, pp. 214–224. doi: 10.1016/j.eswa.2019.03.042.

Kumar, D. (2018) 'PERFORMANCE ANALYSIS OF VARIOUS CREDIT CARD FRAUD DETECTION APPROACHES : A REVIEW', pp. 120–126.

Lucas, Y. *et al.* (2020) 'Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs', *Future Generation Computer Systems*. Elsevier B.V., 102, pp. 393–402. doi: 10.1016/j.future.2019.08.029.

Mandal, P. *et al.* (2016) 'A complete literature review on financial fraud detection applying data mining techniques', *International Journal of Trust Management in Computing and Communications*, 3(4), p. 336. doi: 10.1504/ijtmcc.2016.10005490.

Mînăstireanu, E. *et al.*. (2020) 'Methods of Handling Unbalanced Datasets in Credit Card Fraud Detection', *Brain. Broad Research in Artificial Intelligence and Neuroscience*, 11(1), pp. 131–143. doi: 10.18662/brain/11.1/19.

Misra, S. *et al.* (2020) 'An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction', *Procedia Computer Science*. Elsevier B.V., 167(2019), pp. 254–262. doi: 10.1016/j.procs.2020.03.219.

Mittal, S. *et al.* (2019) 'Computational techniques for real-time credit card fraud detection', *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pp. 653–681. doi: 10.1007/978-3-030-22277-2_26.

Nami, S. *et al.* (2018) 'Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors', *Expert Systems with Applications*. Elsevier Ltd, 110, pp. 381–392. doi: 10.1016/j.eswa.2018.06.011.

Olaechea, D. (2014) *https://www.nerdwallet.com/blog/credit-cards/issued-first-credit-card/, NerdWallet*. Available at: https://www.nerdwallet.com/blog/credit-cards/issued-first-credit-card/ (Accessed: 18 January 2020).

Patil, S. *et al.* (2018) 'Predictive Modelling for Credit Card Fraud Detection Using Data Analytics', *Procedia Computer Science*, 132, pp. 385–395. doi: 10.1016/j.procs.2018.05.199.

Rafiq Ahmed Mohammed, *et al.* (2018) 'Scalable Machine Learning Techniques for Highly Imbalanced Credit Card Fraud Detection: A Comparative Study', *Pacific Rim International Conference on Artificial Intelligence*.

Richardson, J. *et al.* (2020) 'Fraud & security', (May). doi: 10.1016/S1361-3723(20)30045-2.

Rtayli, N. and Enneya, N. (2020) 'Selection Features and Support Vector Machine for Credit Card Risk Identification', *Procedia Manufacturing*. Elsevier B.V., 46, pp. 941–948. doi: 10.1016/j.promfg.2020.05.012.

Ryman-Tubb *et al.* (2018) 'How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark', *Engineering Applications of Artificial Intelligence*. Elsevier Ltd, 76(July), pp. 130–157. doi: 10.1016/j.engappai.2018.07.008.

de Sá *et al.* (2018) 'A customized classification algorithm for credit card fraud detection', *Engineering Applications of Artificial Intelligence*. Elsevier Ltd, 72(October 2017), pp. 21–29. doi: 10.1016/j.engappai.2018.03.011.

Shah, A. *et al.* (2019) 'ONLINE TRANSACTION FRAUD DETECTION MECHANISMS : A', 21(11), pp. 641–646.

Shah, Y. A. *et al.* (2020) 'DETECTING FRAUDS FROM CREDIT CARD TRANSACTION USING IMPROVED', (56).

Song, C. *et al.* (2019) 'Referral reward programs with scarcity messages on bank credit card adoption', *International Journal of Bank Marketing*, 37(2), pp. 531–544. doi: 10.1108/IJBM-12-2017-0260.

Subbulakshmi, T. *et al.* (2010) 'Real Time Classification and Clustering of Ids Alerts Using Machine

Learning Algorithms', *International Journal of Artificial Intelligence & Applications (IJAIA)*, 1(1), pp. 1–9.

Tariq, N. (2018) 'Impact of Cyberattacks on Financial Institutions', *Journal of Internet Banking and Commerce*, 23(2), pp. 1–11. Available at: http://eserv.uum.edu.my/docview/2122484326?accountid=42599.

Vikrant Agaskar, P. *et al.* (2017) 'Unsupervised Learning for Credit Card fraud detection', *International Research Journal of Engineering and Technology*, 4(3), pp. 2395–56. Available at: https://www.irjet.net/archives/V4/i3/IRJET-V4I3608.pdf.

Wang, D. *et al.* (2019) 'Credit card fraud detection strategies with consumer incentives', *Omega (United Kingdom)*. Elsevier Ltd, 88, pp. 179–195. doi: 10.1016/j.omega.2018.07.001.

Younus Ahmad Shah *et al.* (2019) 'Online transaction fraud detection mechanisms: a comparative analysis', *Journal of the Gujarat Research Society*.

Yousefi, N. *et al.* (2019) 'A Comprehensive Survey on Machine Learning Techniques and User Authentication Approaches for Credit Card Fraud Detection', pp. 1–27. Available at: http://arxiv.org/abs/1912.02629.

Zhang, X. *et al.* (2019) 'HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture', *Information Sciences*. Elsevier Inc., (2019). doi: 10.1016/j.ins.2019.05.023.

Zhu, H. *et al.* (2020) 'Optimizing Weighted Extreme Learning Machines for imbalanced classification and application to credit card fraud detection', *Neurocomputing*. Elsevier B.V., 407, pp. 50–62. doi: 10.1016/j.neucom.2020.04.078.