ISSN: 2708-7123 | Volume-**02**, Issue Number-**03** | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

Detecting Mobile Money Laundering Using KPCA as Feature Selection Method

Shamila Bashir[1], Sumira Jabin[2], Saima Jabin[3]
[1]shamilabashir95@gmail.com
[2] sumirajabin786@gmail.com
[3]Saimajabin112@gmail.com

ABSTRACT— In recent years, mobile phone payment systems have been extensively used in developed countries. Frauds are affecting the economy of the whole world. Different kinds of mobile money frauds are credit card, bank fraud, insurance fraud and financial fraud. In this paper, we discussed financial fraud and proposed an effectiveness method for money laundering. Payment system in fraud divided into four parts, point of sale, mobile payment platform, mobile payment independent and bill payment through mobile. Mobile phones are great source of service for financial transactions. Our objective is to identify the misuse of mobile money transaction and to prevent fraud from financial transaction to save the money. Financial Action Task Force (FATF) is an organization that views internationally money laundering. Financial Action Task Force continuously strengthens its standards for dealing with new risks. The Financial Action Task Force monitors countries to ensure the implementation the Financial Action Task Force Standards and holds countries to account that do not comply. This paper proposes hybrid Kernel Principal Component Analysis method used on as feature selection method and investigates the performance of Decision Tree and Boost classification Machine learning method. We applied Area under the ROC curve (AUC) and confusion matrix after using the feature selection method. We found the results of Decision Tree Training, testing and Boost with different Sampling of both datasets and Boost has better performance than Decision Tree.

Keywords— Kernel Principal Component Analysis (KPCA), machine learning (ML), rattle, receiver operating characteristic (ROC).

I.INTRODUCTION

Money laundering (ML) affects the financial affairs of the nations. Money laundering is difficult to detect due to large-scale payment transactions. It is very natural money laundering is an illegal activity. There is no proof for money laundering because accountant, banker and other professional are involved in money laundering. There are many kinds of methods for payments, mobile or wireless credit card readers, mobile wallets, Quick Response (QR) code payment, internet payment, Short Message Service (SMS) payment and many other methods. In this paper author proposed hybrid Kernel Principal Component Analysis method used as feature selection method and studies the performance of Decision Tree and Boost classification Machine learning method. For acquiring the result, Area under the ROC curve (AUC) after using the genetic algorithm as feature selection. We found the result of Decision Tree training, testing and Boost with different Sampling of both datasets.

Mobile payment has been directly security desires with the design of suitable security protocols mobile wallets. But identified yet the possibility level of development; as a result, there is a need to improve the research area or MMT [6]. For detecting fraud in mobile money transaction using data mining techniques. Shahed & Ibrahim et al (2019) used Support vector machine, decision tree and python software with Genetic calculation for confusion matrix. Decision tree used 10020 data for experiment and after the experiment the accuracy is 94% and executing time is 263.8233 sec. the author applied the support vector machine algorithm the accuracy is 96% and executing time 0.493 sec. After applying artificial neural network algorithm the accuracy is 97.83% and executing time 91.12 sec. Among these three algorithms, we see that artificial neural network algorithm gives better accuracy 97.83% but

ISSN: 2708-7123 | Volume-**02**, Issue Number-**03** | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

executing time is 91.12 sec. On the other hand, support vector machine algorithm gives the accuracy 96.14% and the executing time is 0.493 sec. SVM takes very short time for execution. Between the two types of data quantity, we find that artificial neural network gives better accuracy [11]. Monitoring the system doubtfully activity to perform money laundering and other criminal activies. Identification practices embodied in SIM registration and Know Your Customer make mobile money customers and their transactions legible to service providers. Back-end monitoring systems attempt to spot suspicious activity on platforms, though money laundering and other illicit activities persist. Most recently, government has taken a keen interest in more invasive forms of regulatory oversight by directly accessing mobile money platform data; however, this is increasingly driven by concerns about generating tax revenue and not security per se. Scalability challenging to dealing with non-Linearity to graphs of any meaningful size. Dynamic challenges of Anti-Money Laundering (AML) Using synthetic data with Deep Learning Model basic experient result were collected [9]. Kaler & Kanezashi et al (2018) Generated 10 training traces of each type of the behaviour. Experimented using higher number training traces and also generating an unbalanced training set. K-nearest neighbour approaches can obtain good accuracy even in the unbalanced case [13]. In this paper author tested the hypothesis of the learning system and will be able to identify new unseen behaviour. In this case decision tree, also had 100% accuracy, but the average number of observations that it required to converge to the right decision are 50.95%. Experimental results show that CABBOT can learn to classify traces in the presence of different observably models [24].

International organizations, such as the United Nations or the Bank for International Settlements, took some initial steps at the end of the 1980s for detecting money laundering. After the creation of the Financial Action Task Force (FATF) in 1989, the European Union, Council of Europe, Organization of American States, met to name just a few established anti-money laundering standards for their member countries. The Caribbean, Asia, Europe and southern Africa have created regional anti-money laundering task force-like organizations, and similar groupings were planned for western Africa and Latin America in the coming years. Financial Action Task Force (FATF) is an organization that views internationally money-laundering watchdog. Financial Action Task Force continuously strengthens its standards for dealing with new risks. FATF maintain two lists back list and grey list. Countries on its black list are those that not cooperate in global effort to detect the money laundering. On other hand grey list refer to as increasing monitoring and present significant risk of ML. Pakistan has been in grey list since June 2018. Pakistan has made progress across all action plans and has now largely addressed until 21 of the 27 action items. As all action plan deadlines have expired, the FATF strongly urges Pakistan to quickly complete its full action plan by February 2021; it said in a statement 21 February 2020 countries in black list North Korea and Iran [23].

Global recognition Anti-money laundering rules increased when the financial Action Task Force (FATF) was formed because it set the international standards in the fight against the money laundering. Identify the mobile money transaction that is used in money laundering. Provide an alternative method for fraud detection in Mobile Money laundering. That is helpful to develop a system, that are monitoring and analytical models for fraud detection in money laundering. Improve the payment system in the field of business communities and deal with large data set. We have used data mining techniques for fraud detection from large data. Because Data Mining (DM) is a process to extract pattern from large data and convert to useful data. DM has been used in multiple fields like science and research. Therefore, we have collected data from Kaggle and applied data mining techniques. To Detect Mobile Money Laundering we used Kernel Principal Component Analysis as Feature selection with Machine Learning methods. Applied Kernel Principal Component Analysis as feature selection solves the problem of imbalanced data. Machine learning algorithms deal with imbalance data. There is a need to develop a strategy for handling the robust risk of mobile money fraud detection. Fraud detection will give business benefits in terms of reducing cost and new style of operation.

ISSN: 2708-7123 | Volume-02, Issue Number-03 | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

II.LITERATURE REVIEW

Money laundering is a global appearance internationally which is 24 hours a day business. In 1988 banking regulation and supervisor practices started prevention of criminal use of the banking system [22]. Payment system introduced first time in 20th century 1950, when credit card introduced. Electronic payment introduce in 1997, Shofwan (2017). Random forest method is described successfully and applies testable use in the payment area on real world data test building 0.003170 secs, detection o.ooooo3 secs, Alexander Diadiushkin e (2019). Use different methods to detect money laundering. Decision tree method can understand all scenarios of money laundering. Reduce the clusters in monitor's framework, MOHAMED ZAKI (2016).

S-Axelsson and Edgar Alonso have used Multi-Agent-Based simulation approach on real wolrd data for mobile money laundering. Applied confusion matrix with decision tree and random forest for classifiaction. The synthetic data represents a scenario experiement with machine learning. First scenerio with 2000 clients distributed in different 7 cities with multiple edges and in another scenerio 20 accounts in 3 cities, S- Axelsson (2012), Edgar Alonso (2012). Adedoyin and Kapetanakis developed a monitoring and analytical model for fraud transaction and used case- Based- Reasoning (CBR) model. CBR identify the money fraud and better performance with Log information. Applied Genetic algorithm is used as a tool to optimize the level (weight) of the feature with K-Nearest Neighbour (K-NN). Case Based Reasoning (CBR) prediction accuracy is 0.97% and 0.98% for two features, Adedoyin and Kapetanakis (2017). Another approach information and comunication technology (ICT) is speedy to contribute in development and transformation in payment system. Almost 2.5 billion people in the whole world without formal banking accounts in most developing countries, Shofwan (2017).

Wagner recognize Latent representation hat is useful for forecasting to nearby verticles in unplanned sequense. Authors used Deep Walk algorithm a combination of supervised classification Naïve Bayes (NB), support vector machine (SVM) and Multilayaer perceptron (MLP). NB= AUC 0.781 with random duplication of he minority class sample. SVM classifier delivers AUC=0.785 difference between SMOTE AUC of SVM 0.044, Wagner Dominik (2019). Bitmap Index Decision Tree method (BIDT) organizes the rows and columns on the account of the client's facts. BIDT decrease the risk of fraud and handle huge money laundering accounts. True positive rate BIDT technique 8-14% compared to Smart Card-Based Security Framework (SCSF). Improved the true positive rate in BIDT by 12-21% is compared with Multilayered Detection System (MDS), Vikas Jayasree & R.V. Siva Balan (2017).

It is very challenging to implementation on imbalance data and large data. For this purpose used decision tree, KNN and random forest for sampling. Using R, Python and SPSS modeller is the better result. Applied two attributes as a target features and got the different results of classifications methods. Decision tree AUC is 1 the best result, Nitin Bhore & Dr. Shridhar (2020).

In this paper, a hybrid model based on Kernel Principal Component Analysis (KPCA) is used as feature selection method with decision tree and Boost classification to detect mobile money laundering. How to solve huge imbalanced data to detect mobile money fraud? It has been discussed earlier that financial fraud is the biggest enemy of an economy. Mobile money payment services environment, offering basic knowledge on basics of mobile money such as the business model and ecosystem issues. Different applications of Machine Learning methods exist in fraud detection in Mobile money Laundering and main problem is how to handle imbalanced data?

III.METHODOLOGY

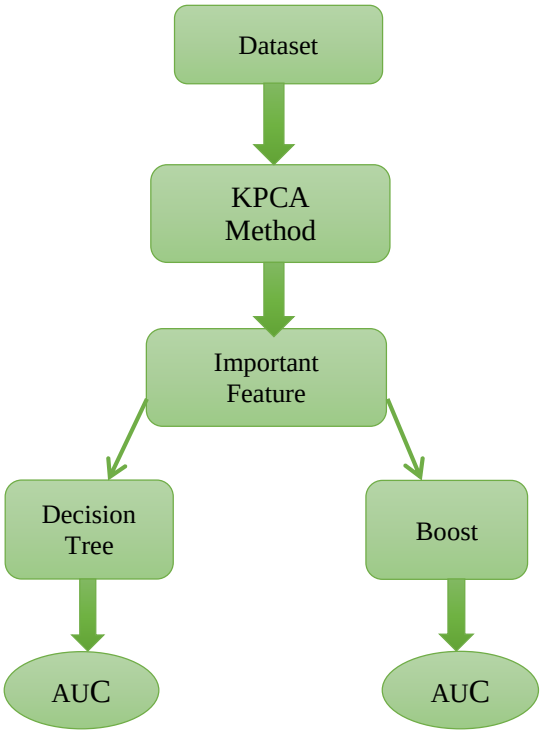
The basic aim of a research methodology is to explain what techniques are being used. Research methodology usually divide into two groups Descriptive and analytical. Descriptive research is related to surveys and studies. Descriptive research aim is to identify the facts. On other hand words descriptive research is state of affairs as it is at present. Analytical research is based on facts or information already available. In this paper used analytical research. A good

ISSN: 2708-7123 | Volume-**02**, Issue Number-**03** | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

research methodology is very important for representing good image [25].

Exploratory Data Analysis for Data Understanding

Theories are developed by researchers to clarify work, draw concepts, and to make a prediction. Framework is based on knowledge, observation, and ideas. Theoretical frameworks where you discuss and evaluate the theories that are most related to your research. Explain the Expectations that guide your work project.



Mobile Money Transaction Data Source.

In this paper used two datasets collected from Kaggle [19]. Kaggle is a machine learning and data science community. It is useful for learning data science and competing with other data users. We used for feature selection Kernel Principal Component Analysis (KPCA), because datasets are exceptionally large. Then we are implementing classification method Decision Tree and Boost with Rattle. In both data sets 0 is donated to non-fraud and 1 is for fraud.

Feature Selection

Principal component analysis (PCA) is a popular tool for linear dimensionality reduction and feature extraction. Kernel PCA is the nonlinear form of PCA, which better exploits the complicated spatial structure of high-dimensional features. PCA attempts to find a linear subspace of lower dimensionality than the original feature space, where the new features have the largest variance [35].

KPCA Performed: In practice, for PCA or KPCA, a re-entering of the data is generally performed. This is because PCA is view as a technique to analyse the variance of the data; it is often desirable to treat the mean independently as a preliminary step [36].

In this paper used the Kernel Principal Component Analysis for feature selection. The Fraud and Exited variable are the target variable. Data Mining Algorithm is described as either descriptive or predictive. Rattle supports two common descriptive or supervised Methods. For Models, building clustering analysis and association analysis are used [16].

Predictive model builders are supported by decision tree and Boost. A confusing matrix is a summary of prediction result on a classification problem. Below is process of calculation a confusion matrix.

1. Need a test dataset with expected outcome value.
2. Make prediction for each row in test dataset.
3. From the expected outcome and prediction counts.
4. Each row of the matrix corresponds to predicted class.
5. Each column of the matrix corresponds to an actual class.

Count of the correct and incorrect classifications is then filling into the table [26]. Receiver Operating Characteristic Curve (ROC) is a graphical plot that is used to show the ability of binary classification. This curve has two parameters.

1. TPR
2. FPR

TPR (True Positive Rate)

$$TPR = \frac{TP}{TP+FN}$$

ISSN: 2708-7123 | Volume-02, Issue Number-03 | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

FPR (False Positive Rate

$$FPR = \frac{FP}{FP + TN}$$

Area under the ROC Curve (AUC) curve plot TPR vs FPR at different classification thresholds. Classification threshold classifier more items as positive and Increasing both false positive and true positive. AUC measure two-dimensional area underneath the entire ROC curve (0, 0) to (1,1) AUC and aggregate measure of performance across all possible classification thresholds [21].

IV. DATA ANALYSIS & RESULTS

Data Mining Algorithm is described as either descriptive or predictive. Rattle supports two common descriptive or supervised Methods. For Models, building clustering analysis and association analysis are used. Predictive model builders are supported by decision tree and Boost. We have used machine learning for getting Area under the ROC curve (AUC) after using the feature selection. We have the result of Decision Tree validation, testing and Boost with different sampling of both datasets.

In this paper used the Kernel Principal Component Analysis as feature selection method with machine learning classification Decision tree and Boost. Using the sampling for classification with validation and testing 70% training 15% validation 15% testing. Secondly sampling size is 70% training and 30% testing. Third sampling is 80% training and 20% testing and same sampling applied with Boost classifier.

Results— First Dataset.

We have found the result of decision tree Training with sampling 70% training 15% validation 15% testing AUC is 1 and with Boost training AUC is 1. Decision tree with sampling of testing 70% Training 15% validation 15% testing AUC is 0.79 and with Boost testing AUC is 0.99. Decision tree with sampling of Testing 70% training 30% testing with training AUC is 1 and Testing AUC is 0.84. With same sampling Boost training AUC is 1 and Boost testing AUC is 0.99. Decision tree with sampling g of 80% training 20% Testing AUC is 1, testing AUC is 0.84 and Boost Training AUC is 1 and Boost testing AUC is 1 [Table 1].

Table 1: First dataset Table

Decision tree and Boost Sampling	Training		Testing	
	AUC Decision Tree	AUC Boost	AUC Decision Tree	AUC Boost
70/15/15	1	1	0.79	0.99
70/0/30	1	1	0.84	0.99
80/0/20	1	1	0.84	1

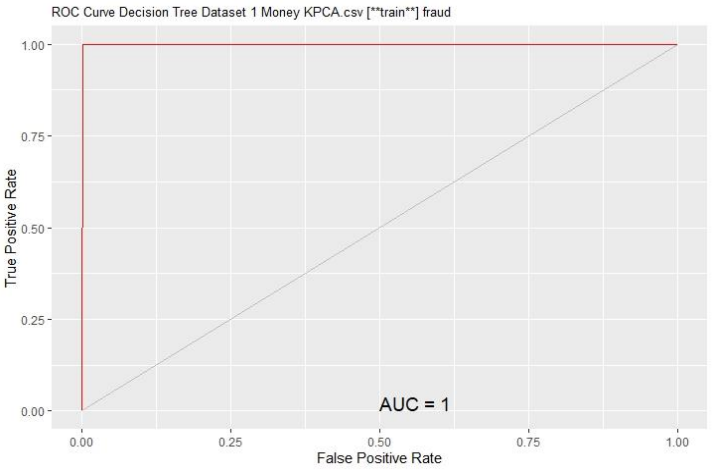


Figure 2: Decision Tree of first dataset

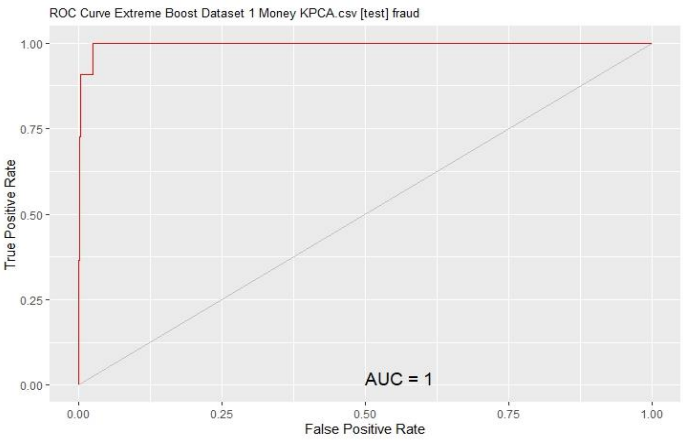


Figure 3: Boost of First Dataset

ISSN: 2708-7123 | Volume-02, Issue Number-03 | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

Second Dataset

We have found the result of decision tree Training with sampling 70% training 15% validation 15% testing AUC is 0.97 and with Boost AUC is 0.99. Decision tree with sampling of testing 70% Training 15% validation 15% testing AUC is 0.55 and with Boost AUC is 0.55. Decision tree with sampling of 70% training 30% testing with training AUC is 0.97 and Testing AUC is 0.54. With same sampling Boost training AUC is 0.99 and Boost testing AUC is 0.84. Decision tree with sampling of 80% training 20% Testing AUC training is 0.98, testing AUC is 0.55 and Boost Training AUC is 0.99 and Boost testing AUC is 0.84.[Table 2].

Table 2: Second Dataset Table

Decision tree and Boost Sampling	Training		Testing	
	AUC Decision Tree	AUC Boost	AUC Decisoon Tree	AUC Boost
70/15/15	0.97	0.99	0.55	0.55
70/0/30	0.97	0.99	0.54	0.84
80/0/20	0.98	0.99	0.55	0.84

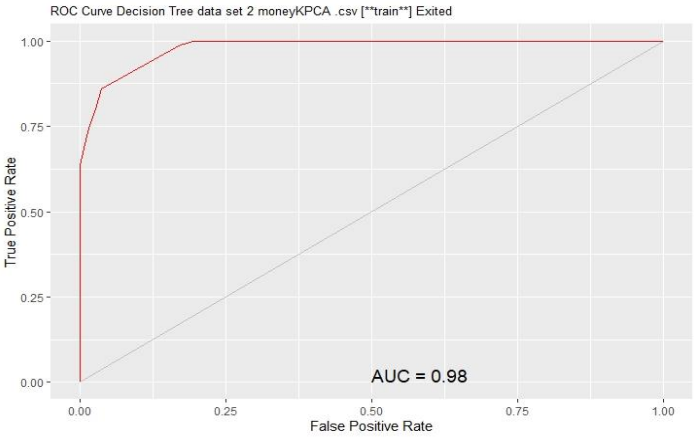


Figure 4: Decision Tree of second dataset

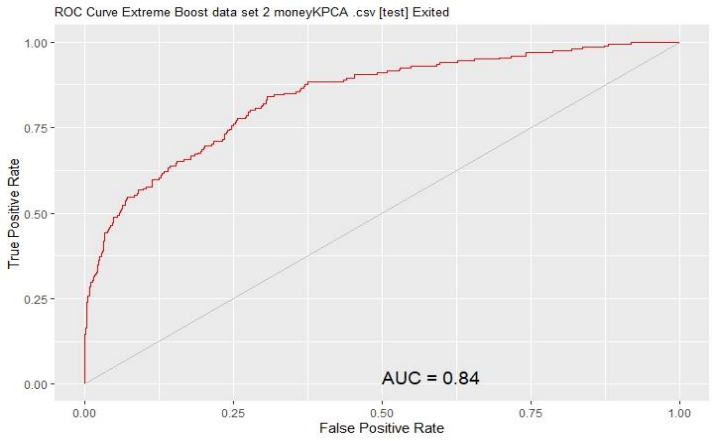


Figure 5: Boost of second dataset

V. DISCUSSION

Fraud in mobile money transfer we understand cash in, cash out national community. It is useful for learning data science and competing with other data users. These datasets we used for feature selection with Kernel Principal Component Analysis (KPCA), because datasets are exceptionally large. Then we are implementing classification Decision Tree and Boost with Rattle. Found the results with Area under the ROC curve (AUC). In this study we thoroughly investigated and international transfer, bill payment. As mobile money laundering is increasing day by day. In this paper used two datasets collected Kaggle. Kaggle is a machine learning and data science mobile payment fraud data to gain insight about which features could be important, also performed data- balancing for both Fraud and Exited target feature. We presented an analysis of the use of a synthetic dataset of mobile money payment for experimentation with machine learning methods. Applied the methods can be used to evaluate the accuracy of different algorithms.

It is discussed that we have found the result of decision tree Training with sampling 70% training 15% validation 15% testing AUC is 1 and with Boost training AUC is 1. Decision tree with sampling of testing 70% Training 15% validation 15% testing AUC is 0.79 and with Boost testing AUC is 0.99. Decision tree with sampling of Testing 70% training 30% testing with training AUC is 1 and Testing AUC is 0.84. With same sampling Boost training AUC is 1 and Boost testing AUC is 0.99. Decision tree with sampling g of 80% training

ISSN: 2708-7123 | Volume-**02**, Issue Number-**03** | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

20% Testing AUC is 1, testing AUC is 0.84 and Boost Training AUC is 1 and Boost testing AUC is 1 [Table 1].

We have found the result of decision tree Training with sampling 70% training 15% validation 15% testing AUC is 0.97 and with Boost AUC is 0.99. Decision tree with sampling of testing 70% Training 15% validation 15% testing AUC is 0.55 and with Boost AUC is 0.55. Decision tree with sampling of 70% training 30% testing with training AUC is 0.97 and Testing AUC is 0.54. With same sampling Boost training AUC is 0.99 and Boost testing AUC is 0.84. Decision tree with sampling of 80% training 20% Testing AUC training is 0.98, testing AUC is 0.55 and Boost Training AUC is 0.99 and Boost testing AUC is 0.84.[Table 2].

Analysed the Decision Tree and Boosting with Training and testing. Decision tree rules that more understandable by human operator than other machine learning algorithms. For imbalanced data, we applied Kernel Principal Component Analysis as feature selection.

KPCA found the important features in data. In both datasets, 0 is donated to non-fraud and 1 is for fraud. Then we applied machine learning methods Decision Tree and Boosting. We presented training and testing the result of this innovative approach. Analytical software tools used for research study are R and rattle modeller methodology. Apply classifier method and compare performance with another Machine Learning algorithm. The simulation of synthetic mobile money dataset can be more explored, and experiments can be made on new Machine Learning methods to obtain better and effective results. We found the result of Decision Tree training, testing and Boost with different Sampling of both datasets and Boost has better performance than Decision Tree.

VI. CONCLUSION

Our analysis covers Decision Tree and Boosting with training and testing. For imbalanced data, we applied Kernel Principal Component Analysis as feature selection. KPCA found the important features in data. We found the result of Decision Tree training, testing and Boost with different Sampling of both datasets and Boost has better performance than Decision Tree.

ACKNOWLEDGMENT

Author would like to express my sincere thankfulness to my Family. Completion of this research could not fulfill without support of my Family.

REFERENCES

[1] Adeyinka Adedoyin1, S. K. (2017). Predicting Fraud in Mobile Money Transfer.

[2] Alexander Diadiushkin1, 2. K. (2019). Fraud Detection in Payments Transactions: Overview of Existing. Complex Systems Informatics and Modeling Quarterly (CSIMQ).

[3] Asongu, S. A. (2013). The impact of mobile phone penetration on African inequality.

[4] Axelsson, E. A.-R. (2012). Multi Agent Based Simulation (MABS) of Financial.

[5] Balan, V. J. (2017). Money laundering regulatory risk evaluation using. ISSN:1815-3852(Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tabs19,

[6] Bosamia, M. P. (2018). Mobile Wallet Payments Recent Potential Threats.

[7] Edwin J. Omol1, *. J. (2016). Mobile Money Payment Acceptance Model in Enterprise. Mara Research Journal of Information Science & Technology.

[8] Lopez-Rojas, S. A. (2012). Money Laundering Detection using Synthetic Data. The 27th annual workshop of the Swedish Artificial Intelligence Society (SAIS).

[9] Martin, A. (2019). Mobile Money Platform Surveillance.

[10] MOHAMED ZAKI, T. S. (2016). DESIGN OF A MONITOR FOR DETECTING. Journal of Theoretical and Applied Information Technology.

[11] Shahed, M. S. (2019). FRAUD DETECTION IN MOBILE MONEY. TRANSACTION: A DATA MINING.

[12] Shofwan. (2017). The Roles of Mobile Payments on Accelerated.

[13] Mark Weber, Jie Chen,Toyotaro Suzumura,Aldo Pareja,Tengfei Ma,Hiroki Kanezashi,Tim Kaler,Charles E. Leiserson & Tao B. Schardl. 2018. "Scalable Graph Learning for Anti-Money." *arXiv:1812.00076v1 [cs.SI] 30 Nov 2018* 7.

[14] Wagner Dominik. 2019. "Latent representations of transaction network graphs in." *Gesellschaft für Informatik (Hrsg.): SKILL 2019*, 12.

[15] Nitin Bhore#1, D. S. ( ). Innovative Approach for Application of Machine Learning Techniques in Mobile Payment Fraud Analytics. *ISSN: 0474-9030 Vol-68, Special Issue-27 (Feb. 2020) SINHGAD INSTITUTE OF MANAGEMENT AND COMPUTER APPLICATION (SIMCA Narhe Technical Campus, Pune, Maharashtra (India) 411041.*, 16.

[16] Williams, b. G. (n.d.). Rattle: A Data Mining GUI for R. *The R Journal Vol. 1/2, December 2009*.

[17] NTNU, T. @. (2017). https://www.kaggle.com/ntnu-testimon/banksim1.

[18] Malit, K. (2018). Bank Customer Churn Prediction. *https://www.kaggle.com/kmalit/bank-customerchurnprediction/data*

[19] https://www.kaggle.com/dataset.

ISSN: 2708-7123 | Volume-**02**, Issue Number-**03** | September-2021
LC INTERNATIONAL JOURNAL OF STEM
Web: www.lcjstem.com | DOI: https://doi.org/10.47150

[20] https://www.sciencedirect.com/topics/engineering/genetic-algorithm.

[21]https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc.

[22]https://www.coursehero.com/file/63129059/Trinidad-Money Laundering-Presentation-3-12-14pdf/.

[23] https://www.fatf-gafi.org/faq/moneylaundering.

[24] Shah, D. B. (November 4, 2020). Simulating and Classifying Behavior in Adversarial Environments Based on Action-State Traces: An Application to Money Laundering. *arXiv:2011.01826v1 [cs.AI] 3 Nov 2020*, 20.

[25] https://research-methodology.net/research-methodology/research-types/

[26]https://machinelearningmastery.com/confusion-matrix-machine-learning/.

[27] Tobbin, P. (2011). Understanding the mobile money ecosystem:. 10th International Conference on Mobile Business.

[28] Caddie Shijia Gao, Dongming Xu. 2009. "CONCEPTUAL MODELLING AND DEVELOPMENT OF AN INTELLIGENT AGENTASSISTED DECISION SUPPORT SYSTEM FOR ANTI-MONEY LAUNDERING." *UQ Business School, University of Queensland, St Lucia, Brisbane, QLD 4072, Australia*.

[29] Zhongfei (Mark) Zhang, John J. Salerno and Philip S. Yu. 2003. "pplying Data Mining in Investigating Money Laundering." 6.

[30] J.Kauffman, Y. A. (2007). The economics of mobile payments: Understanding stakeholder. Electronic Commerce Research and Applications.

[31] Joseph Adjei, P. T. (2012). Understanding the Characteristics of Early and Late Adopters of Technology. International Journal of E-Services and Mobile Applications, 4(2), 37-54, April-June 2012 37.

[32] Ross Gombiro, M. J. (2015). A CONCEPTUAL FRAMEWORK FOR DETECTING. Journal of Governance and Regulation / Volume 4, Issue 4, 2015, Continued - 6.

[33] Edwin J. Omol1, *. J. (2016). Mobile Money Payment Acceptance Model in Enterprise. Mara Research Journal of Information Science & Technology.

[34] Emilie Lundin Barse, E. L. (2003). Synthesizing Test Data for Fraud Detection Systems. Chalmers University of Technology.

[35] Bishop, Christopher M. (ed.). Pattern Recognition and Machine Learning. Springer, Cambridge, U.K., 2006

[36] Zwald3, G. B. (n.d.). Statistical Properties of Kernel Principal.,2007, 39.

BIOGRAPHY

Name: Shamila Bashir

Email: shamilabashir95@gmail.com

Shamila Bashir has received her MCS degree for Virtual University of Pakistan. Now, she has completed M. Phil from Institute of Southern Punjab, Multan, Pakistan.

Research Domain: Data Mining.

Name: Sumira Jabin

Email: sumirajabin786@gmail.com

Sumira Jabin has received her MCS degree for Virtual University of Pakistan. Now, she has completed M. Phil from Institute of Southern Punjab, Multan, Pakistan.

Research Domain: Data Mining.

Name: Saima Jabin

Email: saimajabin112@gmail.com

She is doing M. Phil from Institute of Southern Punjab, Multan, Pakistan.