Credit Card Fraud Detection Using Machine Learning

Vishal Kumar [1*], Dr Ritu Pahwa[2]

[1] M.Tech Scholar, Computer Science & Engineering, Dronacharya College of Engineering, Gurugram, India
[2] Associate Professor, Computer Science & Engineering, Dronacharya College of Engineering, Gurugram, India
*Corresponding Author Email: kumvishal.98@gmail.com

Abstract

To make life better, many mechanisms in modern environment are carried out via the Internet. The economy is expanding yet on the other side, there is a lot of illegal and unauthorised activity carried throughout the country that is seriously hampering that progress. Scam instances, which mislead individuals while also causing economic losses, are just one of them. In realistic conditions, fraud involving credit cards surveillance is the main emphasis of this research. Contrary to earlier eras, the number of credit card scammers is drastically increasing right now. Criminals use various forms of innovation, fake documents, and deception to con others and take their cash. Therefore, it is extremely crucial to discover a solution to these frauds. As technology advances, it becomes harder to keep up with the behaviour and trends of illegal activities. Ai technology, machine learning, as well as other relevant data technology fields have advanced to the point that it is currently feasible to expedite this process and reduce the volume of labour-intensive effort needed in recognizing credit card scams. The user-submitted utilization of credit cards database might be collected initially, then using machine learning approach; it would be split into databases for testing and training purposes. This methodical technique could be utilized by researchers once they have evaluated both the larger information collection and the user-provided available data collection. Enhance the accuracy of the outcome statistics after that. Depending on its exactness and precision, a technology's efficiency is assessed. The results show that XG-Boost and Random Forest techniques have the greatest performance.

Keywords

Credit card; XG-Boost, Fraud Detection, Machine Learning Techniques, Random Forest method.

INTRODUCTION

There has been a significant increase in crime as a consequence of the advancement of cutting-edge technologies and worldwide communication [1]. There are two basic strategies for avoiding fraud: identification and mitigation. Preventative measures serve as an additional layer of defence against fraud assaults. Once prevention has been unsuccessful, detection takes place. As a result, when a fake transaction takes place, recognition aids in detecting it and raising an alarm. Web banking transactions have lately started to accept more card not-present payments for credit or debit card operations. According to the Nilson Report from October 2016, electronic payment platforms contributed more than Thirty one trillion dollar globally in 2015, an increase of 7.3percent from 2014. In 2015, damages from fraud on credit cards grew internationally to twenty one billion dollar, and by 2020, they could exceed Thirty one billion dollars [2]. Unfortunately, there was a sharp rise in suspicious transactions, which has a significant influence on the industry. There are various subcategories of credit card fraud. Card-not-present and Card-present frauds seem to be the two primary fraud categories that might be found in a collection of activities. These two categories may also be divided into behaviour crime, software fraud, thievery fraud, and bankrupt forgery.

The 4 forms of fraudulent activity which falls within the above-mentioned category of Card-Not-Present fraud are the topic of this work, and the authors provide a method for spotting these frauds in real-world settings. This decade's replacement for these kinds of techniques is machine learning, which could also handle massive datasets that are difficult for humans to handle [3]. Supervised and unsupervised learning are the two primary divisions of machine learning approaches. Fraud detection could be carried out either manner, and the database will determine when to employ it. In order to progress under supervision, anomalies must first be classified. Several supervised techniques have been employed in the detection of fraud using credit cards over the past few years. There are two basic techniques to analyse data included in this research: categorical data and quantitative information. Initial data in the database are categorized. By using data cleansing and other simple pre-processing methods, the original data could be processed. In order to do the assessment, the relevant procedures must first be used to convert category information into numerical data. Second, to discover the best algorithm, approaches to machine learning utilize categorical variables. This study compares a wide range of machine learning methods using an effective quality metric for the identification of duplicitous credit card purchases in order to select the best methods for the fraudulent categories.

RELATED WORK

Because finance is such a significant part of human lives today, fraud detection in banks is among the most important parts. As information grows in size in units of Peta Bytes (PB), researchers have integrated a conceptual approach with Hadoop that could rapidly read information and transmit it to an analytic website for fraud detection. This will enhance the efficiency of the analytical site in model development. In this article, researchers mentioned a Big Data assessment model to handle a significant amount of data, solutions for addressing algorithms using machine learning for detecting scam, and discovered their effectiveness on standard database to identify scams on a factual foundation, offering low risk and high customer experience. The goal of this study going forward is to fix the generalization error issue with decision trees and to identify real-time fraud transactions for highly streaming actual data [4].

Bank Loan has had some of the latest expansion in the financial and banking industry. Regrettably, bankers should contend with an increasing ratio of bank lending decline as even more individuals utilize borrowed funds. The majority of people or firms who qualify for this scheme are more valuable than some others. This arrangement allows for the borrower to get modest amounts of cash through a wire transfers or digital payments as required. There aren't many of those that have ever paid back a specific amount of currency later, although they do so periodically. Because of this situation, the banks are experiencing difficulties. Utilizing past data, it would therefore be possible to determine the requirement for foreseeing bank lending errors. Therefore, machine learning may enable the identification for dealing with the existing issue and the danger of failure. The goal of this inquiry is to forecast the difficulty of paying back the loan amount. The research revealed over ten million as per Bank of Taiwan statistics. The classifying mechanism and the cluster of independent characteristics are the focus of the linear regression strategy. The preliminary evaluation yields experimental perspectives of the information in a suitable manner. This research also made use of machine learning techniques to get accurate prediction for selecting the desired users depending on available information. However, most systems struggled to solve the challenge of imbalance with the overdue cases in the datasets [5].

Banks and credit providers should be capable of detecting malicious practices if customers are to prevent getting charged for goods they won't purchase. These problems could be resolved using data science, which is especially important when combined with learning algorithms. This study attempts to show how machine learning could characterise an information gathering through the application of credit card scam preventative measures. The Fraudulent Credit Card Transactions Recognition Dilemma involves creating models of prior purchases with credit cards based on data from transactions that turned out to be fake. This method is then employed to assess the legality of a transaction. The objective is to identify all unauthorized transactions while reducing the number of false positive scam classes. A classic example of segmentation is the identification of credit card scams. The significant mechanisms of this scheme include the framework and pre-processing of big information as well as the utilization of several identification methods, such as the Local Outlier Factor and Isolation Forest algorithm, to Principle Component Analysis transformed Credit Card Transaction statistics. However, this idea is challenging to implement in practise due to the collaboration of banks that are uncertain to share statistics because of market competition, in addition to cos of legislative concerns and the protection of their users' confidentiality [6].

The increased utilisation transactions conducted online makes crime more likely and loses both individuals and the finance community a significant amount of cash. Although there are many illicit practises in the financial sector, internet shoppers are most bothered about and conscious of credit card scams. Therefore, one of the well-known methods experts have developed to prevent the losses caused by these illegal activities is to combat scam attempts using data mining and machine learning approaches. Data mining algorithms were primarily utilised to assess the pattern and characteristics of suspected and non-suspicious activities on the basis of standardized and abnormal statistics. It was possible to seamlessly distinguish between suspected and non-suspicious transactions, nevertheless, utilizing classification models and machine learning techniques. Therefore, machine learning and data mining systems were able to recognize among legitimate and illegitimate activities by looking at the characteristics presented by the information. In order to explain supervised oriented classification, the Bayesian network classifiers, Logistics, Tree Augmented Naive Bayes, Naive Bayes, are utilized. After using standardization and the Principal Component Analysis to pre-process the dataset, all categories beat conclusions drawn without pre-processing the dataset by more than 95.0percentage reliability. However, acquiring real-time credit card crime statistics is a very difficult process [7].

The major objective of this investigation is to identify such scams, which includes high-class data mismatch, data availability, variations in fraudulent type, and significant number of false alarms. Several machine learning-based algorithms for credit card identification are presented in the relevant studies, including the Support Vector Machine, Logistic Regression, Extreme Learning Method, Decision Tree, Random Forest, and XG Boost. However, because of their poor accuracy, modern deep learning techniques must still be used to cut down on fraudulent transactions. The significant advance of deep learning techniques was the main focus of attention. To get effective results, competitive examination of both deep learning and machine-learning methods was done. Using the European card benchmark database for detecting scam, a thorough empirical investigation is conducted. The information was first subjected to a machine learning approach, which somewhat increased the accuracy of fraud detection. In the end, three deep convolution network-based models are employed to increase the efficiency of fraudulent detection. The addition of additional layers greatly increased the detection's accuracy. A detailed experimental examination has been carried out utilising the much latest generations while altering the quantity of hidden levels and epochs. The evaluation of the investigation work shows the improved findings at the optimal reliability, f1-score, precise, and effectiveness curve levels, appropriately. For situations involving credit card identification, the suggested model is more efficient than cutting-edge deep learning and machine learning techniques. Investigators have however carried out experiments utilizing balancing statistics and applied deep learning approaches to lower the false-negative ratio. For the detecting cracks of credit card scam in the actual world, the suggested ways can be put into practise. However, there is still very little utilisation of DL techniques [8].

DATA COLLECTION

Among the most crucial pieces of customer data is information regarding credit cards, which should never be distributed carelessly. The study used the publicly accessible data for the investigation as a consequence of this. The Université Libre de Bruxelles computer vision group's credit card scam database was employed throughout this research. The database includes information about how credit cards were used over the progress of 2 days throughout Europe in September 2013. The data received from this survey totalled 284'807, of which 492 events turned out to be fraudulent. The other transactions were all legitimate. The explanation makes it clear that the facts in question are extremely unbalanced [9]. Datahub.io1 was used to download the dataset. 28 characteristics from the database itself are principle components derived from the outcomes of applying the Principal Component Analysis technique to unique statistics. The principal analytical approach is employed to shield customer information from disclosure. There are two more features, "time" and "amount," making an overall of 30 characteristics [10].

PROPOSED METHODOLOGY

A machine learning approach is suggested by research to identify fraudulent credit card activity in online banking transactions. The volume and complexities of the information make it impractical to analyse false transactions individually. Nevertheless, utilising machine learning may be feasible if sufficiently informative characteristics are provided. The initiative would investigate this theory. With supervised classification algorithm like random forest, it is possible to distinguish among fraudulent and legal credit card transactions to assist us in learning about theft without suffering any financial loss. Figure 1 depicts the proposed system's workflow procedure.

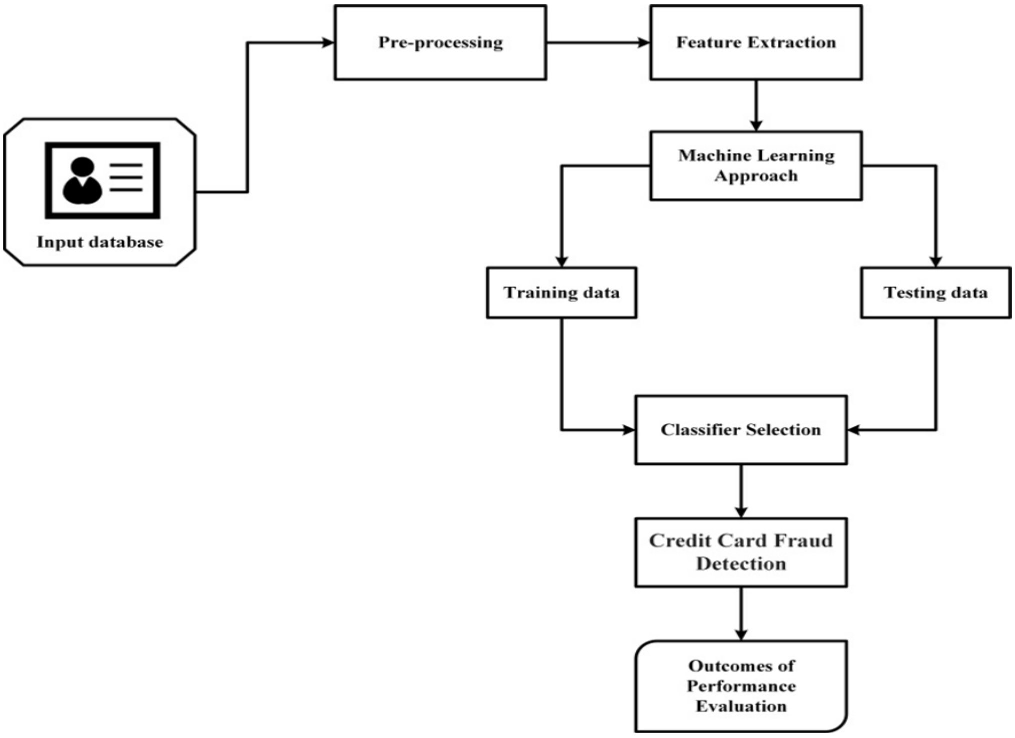


Figure 1. Workflow of the proposed system

Data pre-processing

Data scientists tell a story using the insights they obtain from evaluating and visualizing data. Visualization tool is a way of portraying the data in a graphical and schematic fashion. The best tool in use is Tableau, which offers a tonne of tools for playing with data and producing amazing outcomes. Pre-processing involves the following three crucial and typical steps:

- Sampling: This method of evaluating small samples from larger, more comprehensive dataset may produce better results and aid in comprehending the behaviour and patterns of data in a more comprehensive manner.
- Formatting: It is the method of organizing the data in an appropriate manner so that it can be used. The format of the file systems should really be adjusted as necessary.

- Cleaning: Data cleansing is an essential phase in the machine learning procedure because it takes up the most of the efforts. In addition to simplifying name classifications and other complexities, missing values should be eliminated. For most data analysts, data screening typically makes about 80percent of their workload.

Feature extraction

The process of evaluating the behaviour and pattern of the studied data and generating the characteristics for additional testing and training is referred to as feature extraction. Lastly, the Classification technique is employed to build the classifiers. On the Python Natural Language Toolkit package, researchers use the categorise module. Researchers make use of the acquired labelled database. The algorithms would be assessed using the remaining labelled data we have. Pre-processed data was categorised using a few machine learning methods. Random forest classifications were selected. These methods are frequently used in jobs involving classification task.

Train and test splits

Researchers divided the information into 70 and 30 train and test hold-out validity for the machine learning algorithm. To be even precise, the system educated on the remaining 70 per cent of the data while holding aside 30 per cent of the input as the training dataset. Given the class label, researchers learned the best characteristics using the training set. The test set is a different set that is used to gauge how effectively the system would function with hypothetical data. This strategy guarantees that the model generalises to new scenarios effectively. Since it frequently happens that portions of the testing data may end up leaking into the training data, endangering the system, the train/test divides are independently of one another. Test data are no longer be considered to be unseen information when data leaking happens. The method predicts the model's label or reference level before comparing the outcomes with the trained model's real value to assess the proposed on the testing data. The error metric among the y testing and y forecast is assessed to determine the model's error under the assumption that it is assessing a brand-new data set. How effectively the model operates on the unobserved data is shown by the error measurement.

To determine whether an incoming operation is legitimate or not, the analytic method is used. For detecting fraud, decision tree machine learning and logistic regression methods are used. The algorithm is based on a set of banking credit card data. The study classified fraud detection utilizing two concepts.

Designing analytical model for fraud prediction

To determine whether an incoming operation is legitimate or not, the analytic method is used. For detecting fraud, decision tree machine learning and logistic regression methods are used. The algorithm is based on a set of banking credit card data. The study classified fraud detection utilizing two concepts.

Decision tree algorithm

Both regression trees and classification trees are used in this strategy. A decision tree is built in this case using a classification model. Different components make up the framework of this decision tree, and the root node is the node at the top of the tree. The other non-leaf vertices in the tree stand in for the tests conducted on the characteristic, each subsequent branch for the test's response, and each leaf node for a classifier. These leaf nodes additionally display the categories that the system would provide if it came to that conclusion as its final classification. Consequently, the projection would become apparent after a comprehensive traverse of the decision tree. C4.5, Classification and Regression Tree, and Iterative Dichotomiser 3 are a few instances of decision tree techniques. Through continuous execution, this program controls the unchanging set of information and divides and conquers the major issue into smaller issues [11].

Support vector machine

SVMs, in contrast to other neural network models, primarily depend on the structural risk minimising rather than the empirical risk reduction. Vapnik introduced this method in 1992 to troubleshoot and resolve simply the problem of binary categorization, but it has now been expanded to include non-linear regression as well. These SVMs use a specific kernel function to transfer a set of information to an underlying, very high-dimensional domain, and then identify the hyperplane that maximises the margin among any two categories. The Support Vector Machine difficulties' foundations are those statistics, preferably near the margin. These are referred to as support vectors [12].

Logistic regression

In order to categorise fraud prevention, researchers use logistic regression. The logistic curve is used for fraud identification in logistic regression, a sort of probabilistic statistical categorization algorithm. The univariate logistic curve's equation is

$$L = {exp_{(r_0+r_1u_1)}}\Big/{1 + exp_{(r_0+r_1u_1)}} \qquad (1)$$

The likelihood of class membership could be understood as a value between zero and one provided by the logistic curve. The logistic function could be combined with the logarithmic value as illustrated below to accomplish regression.

$$\log_e\left(\frac{L}{1-L}\right) \qquad (2)$$

Here, $1 - L$ is the likelihood that the tuple will not be in class and L is the likelihood that it will be. The model, though, selects r_0 and r_1 coefficient values that maximise the likelihood of a typically consists.

XG Boost

Chen et al. [13] presented the machine learning technique known as XGBoost, which is centered on tree boosting. Prominent method XGBoost uses additional reinforcement learning with second-order estimation, a gradient-like first order derivation, as well as a hessian second order function.

$$B_{(t)} = \sum_{k=1}^{u} b(x_k, L_k^{(t-1)} + c_t(s_u)) + \partial(c_t) \qquad (3)$$

The regularised objective in Eq. (3) is where $b(\ldots,\ldots)$a loss between target x_k and forecast L_k is. The (s_u) sign stands for input. u is the amount of characteristics and the symbol for the model's difficulty is $\partial(\ldots)$ For the fitted tree $L_k^{(t)} = L_k^{(t-1)} + c_t(s_u)$ where t is the amount of training process iterations, the study employed an additive method.

Random Forest

A technique to machine learning with supervision called the randomized forest tree was developed to deal with regression and classification difficulties. The following pseudo code is used by the random forest method to anticipate fraudulent transactions.

1. Retrieve the test features from the received transaction, utilise the criteria of each decision tree that was generated at random, and save the anticipated outcome (target)
2. Determine the vote totals for each projected output.
3. Analyses the most highly rated projected target obtained from various decision trees as the prediction's end outcome.

RESULT AND DISCUSSION

A significant step in the procedure of developing a framework is prototype assessment. Finding the appropriate framework to explain the information and determining how effectively the proposed framework would function in the future are both aided by this. Since training information could easily produce highly positive and over fitted systems, assessing effectiveness of the designs with training statistics is unacceptable in data science. Assessment techniques like holding out now and cross-validations are employed to test quality of the system and prevent over fitting. The final outcome would be categorised statistics represented in graphical format and in a visualised form. The percentage of accurate projections for the testing dataset is a simple method for determining efficiency. The simple analytical formula is to split the entire amount of projections by the amount of accurate guesses.

Table 1. Efficiency evaluation of the suggested and existing techniques

Sr. No.	Machine Learning Algorithm	Prediction Accuracy of Machine learning Algorithm	Precision
1	Decision Tree	99.926	99.97
2	Logistic Regression	99.92	99.99
3	Random Forest	99.952	99.99
4	SVM	99.938	100
5	XGBOOST	99.949	99.99

Each of the measures, such as accuracy, precision may be used to compare each of the approaches as well as to report on how well they performed. A confusion matrix is a table that lists each potential cases or the number of examples that fall into the various designated types accurately. The confusion matrix of a binary classifier is shown in the table 1. Progressive in the challenge of fraud detection denotes honest transactions, whereas negative denotes dishonest transactions. The graphical representation of the Confusion matrix for the suggested system is displayed in Figure 2.

Accuracy

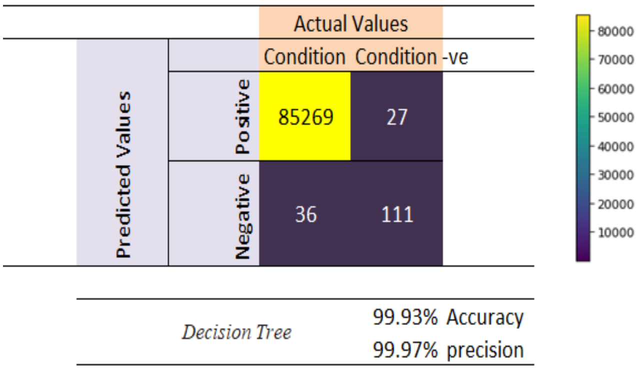
The overall correctness of the suggested method is provided by this variable. Equation (4) demonstrates that it corresponds to the whole quantity of data taken by providing the entire amount of projections.

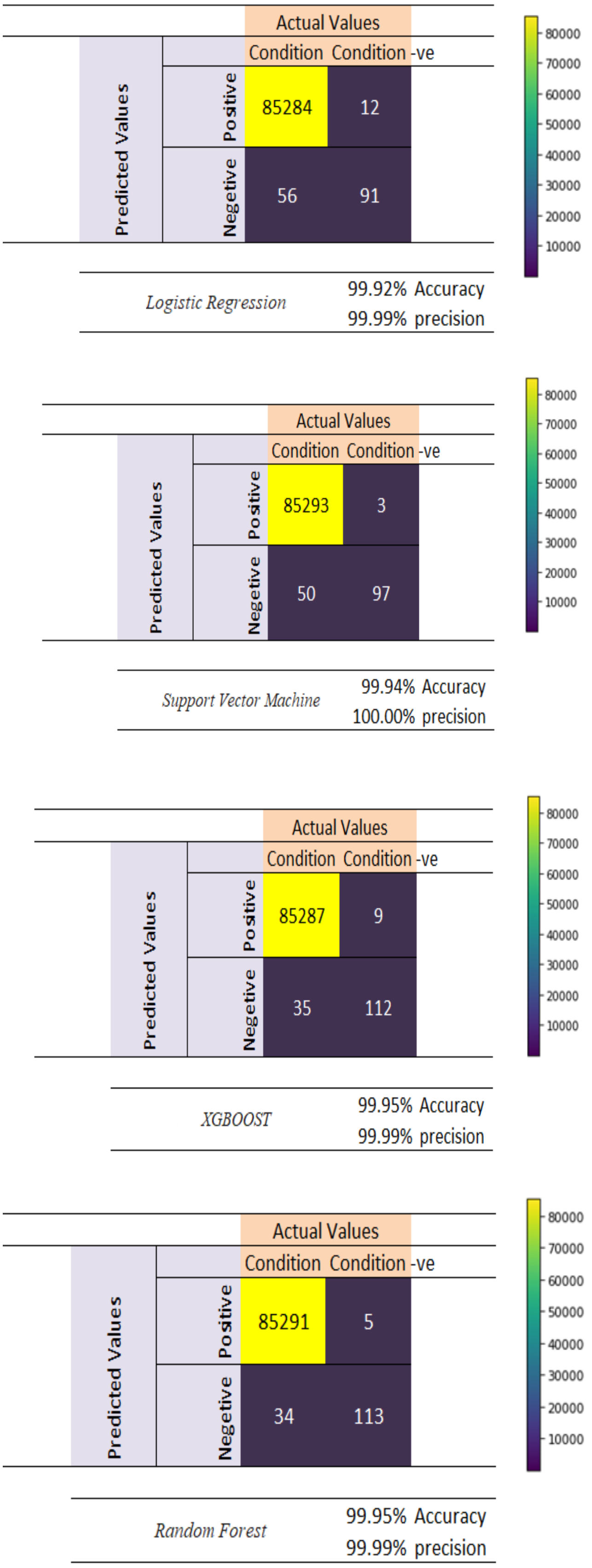
$$Accuracy = \frac{(T_P+T_N)}{(T_P+T_N+F_P+F_N)} \qquad (4)$$

Precision

It is recognized as the percentage of scams which are expected to lead to the exact entire quantity of scam incidences according to Equation (5).

$$Precision = \frac{T_P}{(T_P+F_P)} \qquad (5)$$





		Actual Values	
		Condition	Condition -ve
Predicted Values	Positive	85284	12
	Negetive	56	91

Logistic Regression	99.92% Accuracy 99.99% precision

		Actual Values	
		Condition	Condition -ve
Predicted Values	Positive	85293	3
	Negetive	50	97

Support Vector Machine	99.94% Accuracy 100.00% precision

		Actual Values	
		Condition	Condition -ve
Predicted Values	Positive	85287	9
	Negetive	35	112

XGBOOST	99.95% Accuracy 99.99% precision

		Actual Values	
		Condition	Condition -ve
Predicted Values	Positive	85291	5
	Negetive	34	113

Random Forest	99.95% Accuracy 99.99% precision

Figure 2. Confusion Matrix of Proposed and Existing System

CONCLUSION

Investigators have been involved in the recognition of credit card scams for a long period of time and will likely remain so in the long term. This is mostly caused by the ongoing alteration of fraud behaviours. Utilizing best-fitting algorithms to identify distinct trends of fraudulent payments, it offers a unique credit-card fraud prevention method in this study. This study also addresses relevant issues raised by prior studies on credit card fraud recognition. Therefore, it possesses the ability to calculate accurately to recognize credit cards scam utilizing machine learning techniques. As a consequence, the study's utilization of the random forest method and the upgraded XG-Boost model yielded an exact estimate of identifying credit card fraud of 99.99 per cent. This suggested system offers more reliable analysis than the existing systems and is suitable to a wider database.

REFERENCES

[1] D. Sisodia, K. R. Nerella, and S. Bhandari, “Performance evaluation of class balancing techniques for credit card fraud detection,” Sep. 2017, pp. 2747–2752. doi: 10.1109/ICPCSI.2017.8392219.

[2] Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, “Deep learning detecting fraud in credit card transactions,” Apr. 2018, pp. 129–134. doi: 10.1109/SIEDS.2018.8374722.

[3] R. Choudhary and H. Gianey, “Comprehensive Review On Supervised Machine Learning Algorithms,” Dec. 2017, pp. 37–43. doi: 10.1109/MLDS.2017.11.

[4] S. Patil, V. Nemade, and P. K. Soni, “Predictive Modelling For Credit Card Fraud Detection Using Data Analytics,” *Procedia Comput. Sci.*, vol. 132, pp. 385–395, 2018, doi: 10.1016/j.procs.2018.05.199.

[5] S. Arora, S. Bindra, S. Singh, and V. Kumar Nassa, “Prediction of credit card defaults through data analysis and machine learning techniques,” *Mater. Today Proc.*, vol. 51, pp. 110–117, 2022, doi: 10.1016/j.matpr.2021.04.588.

[6] S. P. Maniraj, A. Saini, S. D. Sarkar, and S. Ahmed, “Credit Card Fraud Detection using Machine Learning and Data Science,” *Int. J. Eng. Res.*, vol. 8, no. 09.

[7] O. S. Yee, S. Sagadevan, and N. H. A. H. Malim, “Credit card fraud detection using machine learning as data mining technique,” *J. Telecommun. Electron. Comput. Eng. JTEC*, vol. 10, no. 1–4, pp. 23–27, 2018.

[8] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms,” *IEEE Access*, vol. 10, pp. 39700–39715, 2022.

[9] D. Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, “Calibrating Probability with Undersampling for Unbalanced Classification,” in *2015 IEEE Symposium Series on Computational Intelligence*, Dec. 2015, pp. 159–166. doi: 10.1109/SSCI.2015.33.

[10] H. Tingfei, C. Guangquan, and H. Kuihua, “Using Variational Auto Encoding in Credit Card Fraud Detection,” *IEEE Access*, vol. 8, pp. 149841–149853, 2020, doi: 10.1109/ACCESS.2020.3015600.

[11] Y. Abakarim, M. Lahby, and A. Attioui, “An efficient real time model for credit card fraud detection based on deep learning,” in *Proceedings of the 12th international*

conference on intelligent systems: theories and applications, 2018, pp. 1–7.

[12] X. Li *et al.*, "Transaction Fraud Detection Using GRU-centered Sandwich-structured Model," in *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*, May 2018, pp. 467–472. doi: 10.1109/CSCWD.2018.8465147.

[13] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA, Aug. 2016, pp. 785–794. doi: 10.1145/2939672.2939785.