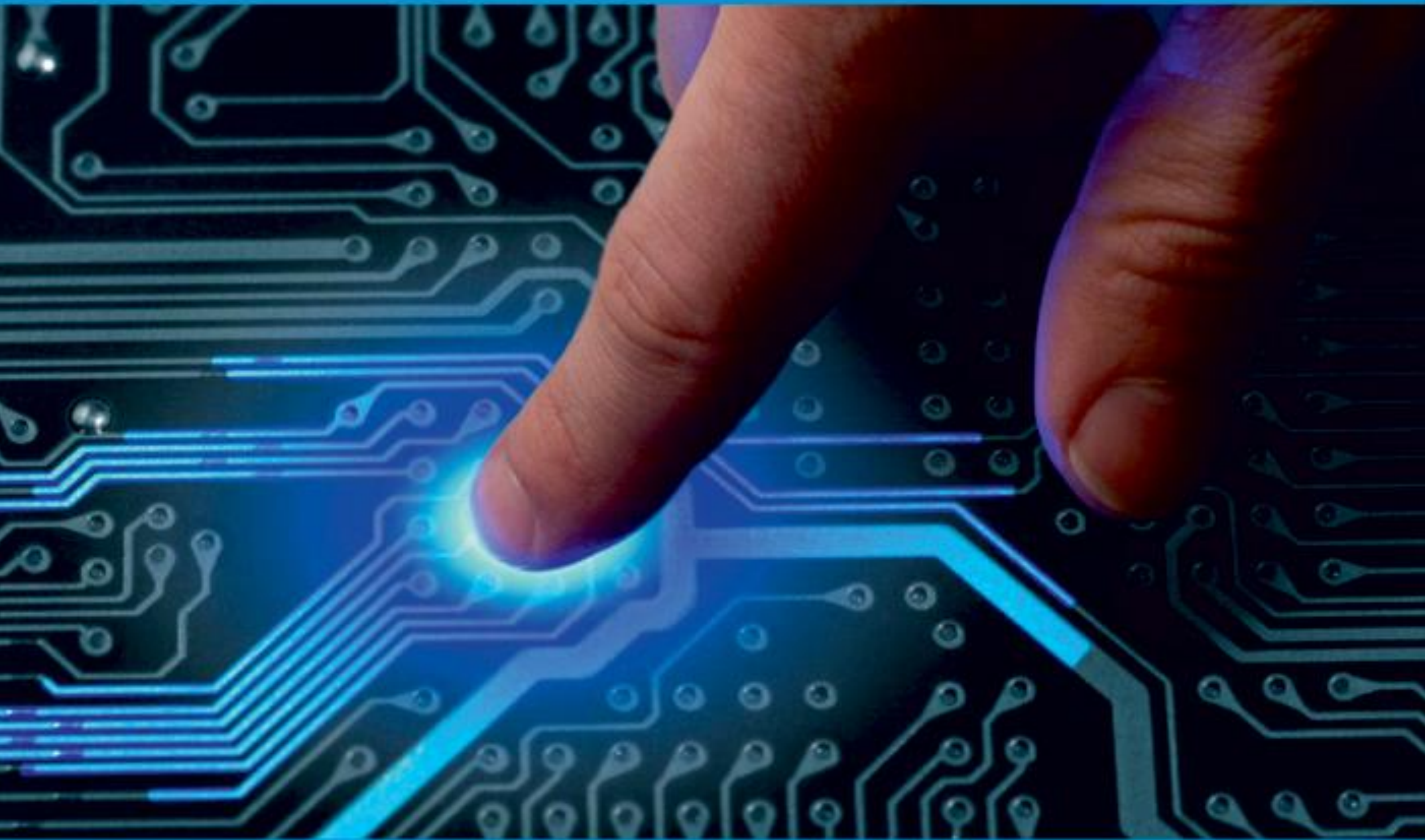
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

Credit Card Fraud Detection Using SVM Algorithm

Mr.T.Anto Theepak, S.Devakingston

Associate Professor, Department of IT, Francis Xavier Engineering College, Tirunelveli, India

B. Tech Student, Department of IT, Francis Xavier Engineering College, Tirunelveli, India

ABSTRACT: The paper largely concentrates on determining actual credit card theft. Due to the phenomenal increase in credit card usage, there has been a substantial boost in counterfeit activity in recent years. The intention is to take something or to make a withdrawal without paying for it funds without permission from a source. All credit card issuing institutions must now put in place to robust fraud detection technologies in a bid to reduce their liabilities. Among the main challenges for the company is the need both the card and the cardholder are not must being there during the transaction. Due of this, it is difficult for the retailer to confirm that the person using a transaction is truly the customer. Using the suggested plan and the SVM technique, With the suggested method and the SVM algorithm, it is possible to improve fraud detection's precision. Analysis of the user's current dataset and the data set under classification is done by the SVM method. Finalize the accuracy of the outcome data. On the basis of a technique's accuracy, sensitivity, specificity, and precision, its effectiveness is determined. Following the some of the processing of the required characteristics, fraud prevention is discovered, and an information visualization portrayal is offered. On the basis of a method's accuracy, sensitivity, specificity, and precision, its effectiveness is evaluated.

I. INTRODUCTION :

Several fraud detection strategies were employed for credit card transactions, including techniques to create models utilizing Machine learning, fuzzy logic, artificial intelligence, and data mining. Finding fraud with credit cards is a frequent issue that can be challenging be resolved. In our suggested remedy, we created the fraudulent using support vector machines to identify credit cards (SVM). The field using machine learning has progressed. Machine learning-based detecting fraud approaches have been discovered. A huge quantity is a data set transmitted throughout processing transactions online, yielding the binary outcome of valid or fraudulent. The example fake datasets are used to develop features. These really are reference points, such as the credit card dataset for the customer account's age, value, and country of origin. There seem to be numerous of qualities, and every single one influences the chance of deception to varying degrees. Be aware that the machine's artificial intelligence, which is fueled by the training set, determines the extent to which each attribute contributes to the fraud score rather than a fraud analyst. Indeed, if it can be shown that using cards to commit fraud is common, the transaction's fraud weighting including with a credit card identical. The level of contribution would, however, parallel if this were to decrease. Simply create these models so they can learn on their own without explicit programming or manual review. When employing automated detection of credit card fraud, classification and regression techniques when utilized. To categories fraudulent use of cards made either online or offline, we employ supervised learning algorithms like the SVM. Regressions and classification Support Vector Machine, or SVM, one of the most popular supervised learning approaches, is used to solve problems. Nevertheless, Machine Learning Classification issues are where it is most frequently employed. So as to quickly categories fresh information in the long term, the SVM algorithm seeks to identify the ideal border or line that can split enter imensional space categories Motivation and Problem Statement.

The pervasive adoption of cloud computing has ushered in unparalleled convenience for remote data management, yet it has concurrently intensified concerns over security and privacy. Cloud services, while offering unprecedented flexibility and scalability, remain susceptible to a myriad of cyber threats, with data loss and leakage standing out as paramount concerns. The inherent reliance on third-party providers introduces a layer of vulnerability, potentially exposing enterprises to significant data breaches and subsequent financial and reputational damage. Moreover, the potential for malicious actors to erase or misuse data stored on remote servers amplifies the urgency for robust security measures. Addressing these challenges head-on, the motivation for this project stems from the imperative to fortify cloud computing infrastructures against these vulnerabilities and protect sensitive data from unauthorized access, tampering, or exploitation. Thus, the problem statement revolves around developing comprehensive solutions that bolster cloud

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

security mechanisms, mitigate the risk of data loss or leakage, and safeguard the privacy of individuals and organizations utilizing cloud services.

1.2 Research Objectives and Contributions:

The research objectives (RO) and research contributions (RC) of the research work are presented as follows:

RO1- Develop an efficient and accurate credit card fraud detection system.
RC1:- Proposed a novel credit card fraud detection framework leveraging state-of-the-art machine learning and deep learning techniques.
RO2- Explore various feature selection and engineering techniques to optimize SVM performance for fraud detection.
RC2:- Explored novel feature selection and engineering methods specifically tailored for SVM-based fraud detection.
RO3- Assess the impact of different kernel functions and parameters on SVM's ability to detect fraudulent transactions. Evaluate the interpretability of SVM models for stakeholders to understand and trust the decision-making process.Compare the performance of SVM with other machine learning and deep learning algorithms commonly used in fraud detection.
RC3:- Conducted extensive experiments to analyze the impact of kernel functions and hyperparameters on SVM's performance. Provided insights into the interpretability of SVM models, facilitating better understanding and trust among stakeholders.Compared SVM's performance with other state-of-the-art fraud detection algorithms, contributing to the understanding of its efficacy in real-world scenarios.

1.3 Proposed Methodology:

The dataset for credit cards is categorised in the proposed model using a support vector machine method. It is the vector machine used to assist supervised learning systems used to solve classification and regression issues. SVM is an algorithm that highly favouredby many people since it generates observable correctness with minimal processing power. SVM is a classification and regression algorithm. The benefit of SVM is because it corrects overfitting to the training set performance. Support vector machines are particularly popular because they produce observable correctness while using minimal processing power. In an N- dimensional space, locating a hyperplane that categorizes the data snippets with clarity is the SVM technique's goal. The amount of characteristics size of the hyperplane is impacted. SVM works well on out-of-sample data and extrapolates well. SVM demonstrates speed because it performs well on out-of-generalization sample data. This is because in SVM, the kernel function is assessed and performed for each and everysupport vector while classifying a single sample. It is mostly used for classification-related problems. There are three different three types of learning: supervised learning, reinforcement learning, unsupervised learning. [9]. A Support vector technology is correctly referred to as a selective classifier since it partitions the hyperplane.

II. RELATED WORK

This section reviews some of the literature published between the year 2020 the year 2024

The identification of card fraud represents one of the successful data processing fields where machine learning techniques play a significant role. Numerous methods for detecting fraud have been developed via earlier research, including supervised procedures, unsupervised strategies, and a mixed approach . We focused on a variety of methods, such as fuzzy logic-based systems, support vector computers, logistic regression, artificial immune systems, neural networks, and K-nearest neighbour, simple bayes, evolutionary Decision trees, algorithms, data mining, and regression. In which we give a theoretical justification for each of six data mining methods (categorization, grouping, forecasting, spotting outliers, regression, and visualization) . Then, we discussed a few of the most recent using computational and statistical techniques like the Artificial Immune System (AIS), Bayesian Belief Network, Neural Network, Support Vector Machine, Logistic Regression, Tree, Self-Organizing Map, and Hybrid Techniques. We got to the judgment that every single aforementioned using machine learning now in use can give high detection rate accuracy, and companies are always looking for innovative ways to enhance their revenue and decrease their expenses. The secret to spotting card fraud is to analyse card activities during purchases. The number of techniques were employed to detect card theft, including synthetic neural networks (ANN), Genetic algorithms (GA), Support vector machines (SVM), product set mining is common (FISM), decision trees (DT), optimization algorithms concerning migrating birds (MBO), procedures for gullible Baiyes (NB). It is used to do out naïve bays analysis and quantitative logistic regression. The output of neural and Bayesian systems is assessed utilizing information about Bank cards theft .

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

2.2 SUMMARY:

Credit card fraud poses a significant challenge for financial institutions and consumers alike. This research focuses on developing an effective fraud detection system using the Support Vector Machines (SVM) algorithm. SVM is a powerful supervised learning method known for its ability to classify data by finding the optimal hyperplane that maximizes the margin between classes.The research begins by outlining the objectives, which include assessing SVM's effectiveness in fraud detection, exploring feature selection and engineering techniques, analyzing kernel functions and parameters, evaluating scalability, addressing robustness against evolving fraud tactics, examining interpretability, and comparing SVM's performance with other algorithms.

To achieve these objectives, the research conducts comprehensive experiments using real-world credit card transaction datasets. Various feature engineering methods are explored to enhance SVM's performance, including dimensionality reduction techniques and feature scaling. The impact of different kernel functions, such as linear, polynomial, and radial basis function (RBF), is investigated to determine the optimal choice for fraud detection.Furthermore, the research addresses the challenge of class imbalance inherent in fraud detection datasets by employing techniques such as oversampling, undersampling, and synthetic data generation. The scalability of SVM is evaluated to ensure its efficiency in processing large volumes of transactions in real-time.To enhance SVM's robustness, the research investigates techniques for adapting to evolving fraud patterns and defending against adversarial attacks. Interpretability analysis is conducted to provide insights into SVM's decision-making process, enabling stakeholders to understand and trust the system's outputs.

Finally, the research compares SVM's performance with other machine learning algorithms commonly used in fraud detection, such as logistic regression, random forests, and neural networks. Through rigorous experimentation and analysis, the study contributes valuable insights into the effectiveness of SVM for credit card fraud detection and its potential applications in real-world scenarios.

III. METHODOLOGY

The methodology for credit card fraud detection using the Support Vector Machines (SVM) algorithm begins with the collection of a diverse dataset containing historical credit card transactions. Following data preprocessing to address missing values, duplicates, and class imbalance, feature engineering techniques are applied to extract relevant information and enhance feature discriminatory power. The SVM algorithm is then implemented, with experimentation conducted on various kernel functions and hyperparameters. Cross-validation ensures model generalization, while parameter tuning optimizes SVM performance. Evaluation on a separate validation dataset assesses real-world performance, complemented by interpretability analysis and comparison with baseline models. Robustness testing against evolving fraud patterns and scalability assessment complete the methodology, culminating in comprehensive documentation and reporting of findings and recommendations.

Following the SVM model's implementation, the next step involves rigorous evaluation to validate its effectiveness in detecting credit card fraud. This evaluation encompasses various aspects, including performance metrics such as precision, recall, F1-score, and area under the Receiver Operating Characteristic (ROC) curve. Through cross-validation techniques, the model's generalization capabilities are assessed, ensuring it can accurately classify fraudulent and legitimate transactions across different subsets of the data. Additionally, the model undergoes scrutiny for robustness against overfitting, as well as sensitivity to changes in hyperparameters and feature selection. Interpretability analysis sheds light on the decision-making process of the SVM model, offering insights into the features driving fraud detection decisions and enhancing trust in its outputs. Moreover, comparative analyses with other state-of-the-art fraud detection algorithms provide valuable benchmarks for evaluating the SVM model's performance and identifying areas for improvement.

3.1 Data Collection:

Acquire a comprehensive dataset containing historical credit card transactions, including both legitimate and fraudulent instances. Ensure the dataset covers a diverse range of transaction types, amounts, and time periods.

3.2 **Data Preprocessing:** Perform preprocessing steps to clean and prepare the dataset for training. This includes handling missing values, removing duplicates, and standardizing features. Additionally, address class imbalance by applying techniques such as oversampling, under sampling, or synthetic data generation .Secure Data Deletion Framework Development:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

3.3 Feature Engineering: Conduct feature engineering to extract relevant information from the dataset and enhance the discriminatory power of the features. Explore techniques such as PCA for dimensionality reduction, feature scaling, and creating new features based on domain knowledge.Smart Contract Implementation.

3.4 Model Training:
Implement the SVM algorithm using appropriate libraries or frameworks such as scikit-learn or TensorFlow. Experiment with different kernel functions (linear, polynomial, RBF) and hyperparameters to optimize the SVM model's performance for fraud detection

3.5 Cross-Validattion:
Perform k-fold cross-validation to evaluate the SVM model's generalization performance and assess its robustness against overfitting. Use metrics such as precision, recall, F1-score, and ROC-AUC to measure performance.

3.6 Parameter Tuning:
Utilize techniques such as grid search or random search to fine-tune SVM's hyperparameters, including the choice of kernel function, regularization parameter (C), and kernel-specific parameters (e.g., gamma for RBF kernel).

3.7 Model Evaluation:
Evaluate the trained SVM model on a separate validation dataset to assess its performance in real-world scenarios. Analyze confusion matrices and ROC curves to understand the model's ability to correctly classify fraudulent and legitimate transactions.

3.8 Scalability Testing:
Evaluate the scalability of the SVM-based fraud detection system to ensure its efficiency in processing large volumes of transactions in real-time. Measure processing time and resource utilization under varying workloads.

3.9 Documentation and Reporting:
Document the entire methodology, including data preprocessing steps, feature engineering techniques, model training procedures, and evaluation metrics. Prepare a detailed report summarizing the findings, insights, and recommendations for stakeholders.

3.10 Methodology:
The methodology for credit card fraud detection using the Support Vector Machines (SVM) algorithm involves several key steps to ensure the development of an effective and robust fraud detection system. Firstly, a comprehensive dataset containing historical credit card transactions is collected, encompassing both legitimate and fraudulent instances. Following data collection, preprocessing steps are applied to clean and prepare the dataset, addressing issues such as missing values, duplicates, and class imbalance through techniques like oversampling or undersampling. Feature engineering techniques are then employed to extract relevant information and enhance the discriminatory power of the features, which may include dimensionality reduction using Principal Component Analysis (PCA) and feature scaling.

Subsequently, the SVM algorithm is implemented using appropriate libraries or frameworks, with experimentation conducted on different kernel functions (e.g., linear, polynomial, Radial Basis Function) and hyperparameters. Cross-validation is performed to assess the model's generalization performance and mitigate overfitting, utilizing evaluation metrics such as precision, recall, and F1-score. Parameter tuning techniques such as grid search or random search are employed to optimize SVM's hyperparameters.

The trained SVM model is evaluated on a separate validation dataset to assess its real-world performance, with confusion matrices and ROC curves analyzed to understand its classification capabilities. Interpretability analysis is conducted to gain insights into the model's decision-making process, and comparisons are made with baseline models such as logistic regression and random forests.

Credit card fraud poses a significant challenge for financial institutions and consumers alike. This research focuses on developing an effective fraud detection system using the Support Vector Machines (SVM) algorithm. SVM is a powerful supervised learning method known for its ability to classify data by finding the optimal hyperplane that maximizes the margin between classes.The research begins by outlining the objectives, which include assessing SVM's effectiveness in fraud detection, exploring feature selection and engineering techniques, analyzing kernel functions and parameters, evaluating scalability, addressing robustness against evolving fraud tactics, examining interpretability, and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

comparing SVM's performance with other algorithms.

To achieve these objectives, the research conducts comprehensive experiments using real-world credit card transaction datasets. Various feature engineering methods are explored to enhance SVM's performance, including dimensionality reduction techniques and feature scaling. The impact of different kernel functions, such as linear, polynomial, and radial basis function (RBF), is investigated to determine the optimal choice for fraud detection.Furthermore, the research addresses the challenge of class imbalance inherent in fraud detection datasets by employing techniques such as oversampling, undersampling, and synthetic data generation. The scalability of SVM is evaluated to ensure its efficiency in processing large volumes of transactions in real-time.To enhance SVM's robustness, the research investigates techniques for adapting to evolving fraud patterns and defending against adversarial attacks. Interpretability analysis is conducted to provide insights into SVM's decision-making process, enabling stakeholders to understand and trust the system's outputs.

Finally, the research compares SVM's performance with other machine learning algorithms commonly used in fraud detection, such as logistic regression, random forests, and neural networks. Through rigorous experimentation and analysis, the study contributes valuable insights into the effectiveness of SVM for credit card fraud detection and its potential applications in real-world scenarios.

Data normalization was used, and findings from Random Forest onfraud detection were achieved. Using normalized data and training a random forest on the data will yield good results. Based on supervised learning, the Random Forest algorithm was developed. Finding novel techniques for fraud detection and improving results accuracy are important.For random forest algorithms, there seem to be three essentials hyper - parameters things must be set up prior to training. The quantity of nodes, trees, and sampled characteristics are a few of them. When dealing with classification or regression issues, the random forest classifier may be utilized.

The dataset for credit cards is categorised in the proposed model using a support vector machine method. It is the vector machine used to assist supervised learning systems used to solve classification and regression issues. SVM is an algorithm that highly favouredby many people since it generates observable correctness with minimal processing power. SVM is a classification and regression algorithm. The benefit of SVM is because it corrects overfitting to the training set performance. Support vector machines are particularly popular because they produce observable correctness while using minimal processing power. In an N- dimensional space, locating a hyperplane that categorizes the data snippets with clarity is the SVM technique's goal. The amount of characteristics size of the hyperplane is impacted. SVM works well on out-of-sample data and extrapolates well. SVM demonstrates speed because it performs well on out-of-generalization sample data. This is because in SVM, the kernel function is assessed and performed for each and everysupport vector while classifying a single sample. It is mostly used for classification-related problems. There are three different three types of learning: supervised learning, reinforcement learning, unsupervised learning. [9]. A Support vector technology is correctly referred to as a selective classifier since it partition the hyperplane..

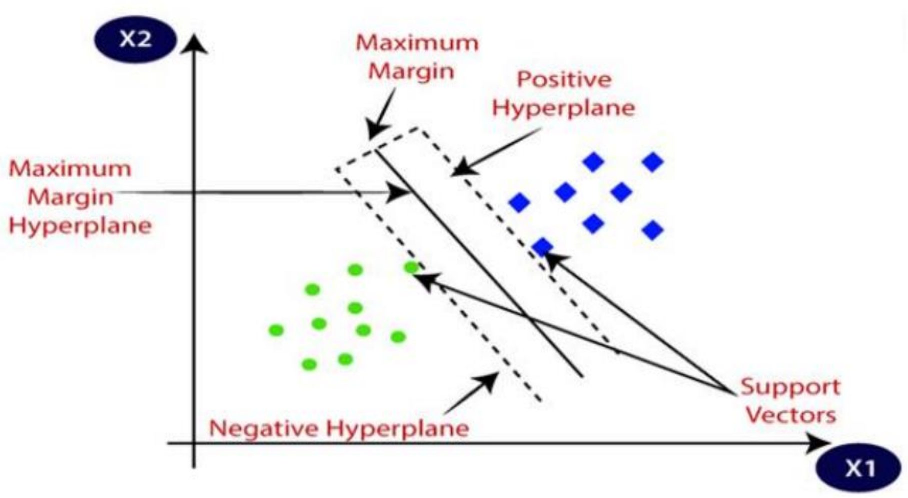


Fig. 3.1: System Architecture – Support Vector Machine Algoritm

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

Classification and regression problems are addressed using SVM, a popular Supervised Learning approach. It is frequently as a tool for machine learning to deal with categorization problems. The optimal judgement boundary or line for categorizing n-dimensional space is soughtfor by the SVM technique so as to quickly add new information to the relevant category. A hyperplane is the ideal boundary that might be chosen. The hyperplane is constructed using the extreme vectors and points selected using SVM. This method, sometimes referred to as the Support Vector Machine, makes use of support vectors. See how two distinct groups are divided by a decision boundary or hyperplanein the figure below. Consequently, the SVM approach assists in locating the best decision boundary or area, sometimes referred to as a hyperplane. The nearest line from each class is identified bythe SVM algorithm. These points are referred to as vectors of support. The margin is separation between the both the hyperplane and vectors. SVM aims to increase this margin. The hyperplane with the biggest margin is the optimum one.

3.11 DATASET:

A collection of facts that a computer considers to be a single thing" is the definition of a dataset. A training algorithm is possible on data set containing many distinct single pieces of the data to find predictable patterns throughout the entire dataset. Despite the dataset's diversity, it may be utilized to teach an algorithm to search for anticipated patterns throughout the whole collection of data.

3.12 EXISTING SYSTEM:

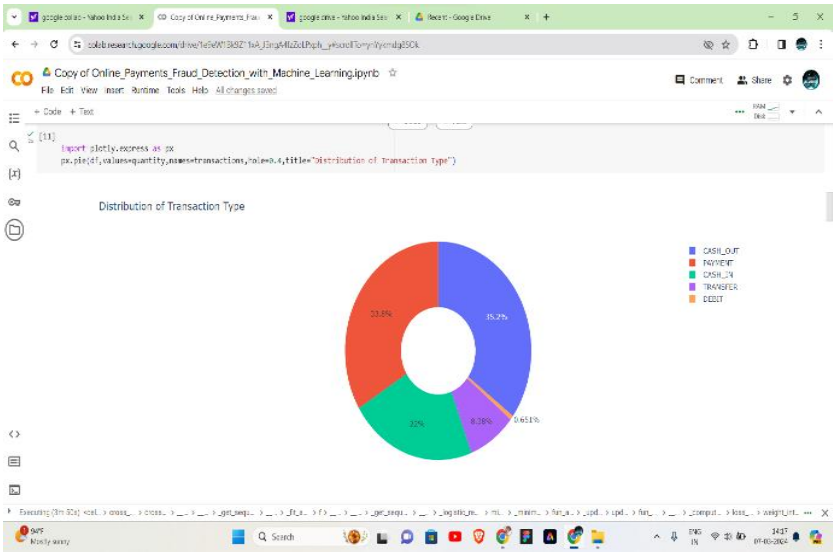
In Random Forest, a method for regression and classification. It's indeed, inessence, a collection of decision tree classification algorithms. The case research involving detection of credit card fraud in the existing system has shown that inputs may be reduced by combining characteristics.

Data normalization was used, and findings from Random Forest onfraud detection were achieved. Using normalized data and training a random forest on the data will yield good results. Based on supervised learning, the Random Forest algorithm was developed. Finding novel techniques for fraud detection and improving results accuracy are important.

For random forest algorithms, there seem to be three essentials hyper - parameters things must be set up prior to training. The quantity of nodes, trees, and sampled characteristics are a few of them. When dealing with classification or regression issues, the random forest classifier may be utilized.

Each decision tree in the ensemble that makes up the random forest method is built using the bootstrap sample, a data sample acquired from a training set with replacement known as the random forest methodology. The out-of-bag sample (oob), which is another name for the training sample, is made up of one-third test data.

Results:



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

```
[12] df=df.dropna()
```

```
df
```

	step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
0	1	PAYMENT	9839.64	C1231006815	170136.00	160296.36	M1979787155	0.00	0.00	0	0
1	1	PAYMENT	1864.28	C1666544295	21249.00	19384.72	M2044282225	0.00	0.00	0	0
2	1	TRANSFER	181.00	C1305486145	181.00	0.00	C553264065	0.00	0.00	1	0
3	1	CASH_OUT	181.00	C840083671	181.00	0.00	C38997010	21182.00	0.00	1	0
4	1	PAYMENT	11668.14	C2048537720	41554.00	29885.86	M1230701703	0.00	0.00	0	0
...	...	...	...	...	...	...	...	...	...	...	...
6362615	743	CASH_OUT	339682.13	C786484425	339682.13	0.00	C776919290	0.00	339682.13	1	0
6362616	743	TRANSFER	6311409.28	C1529008245	6311409.28	0.00	C1881841831	0.00	0.00	1	0
6362617	743	CASH_OUT	6311409.28	C1162922333	6311409.28	0.00	C1365125890	68488.84	6379898.11	1	0
6362618	743	TRANSFER	850002.52	C1685995037	850002.52	0.00	C2080388513	0.00	0.00	1	0
6362619	743	CASH_OUT	850002.52	C1280323807	850002.52	0.00	C873221189	6510099.11	7360101.63	1	0

6362620 rows × 11 columns

S.No	Name of the Algorithm	Accuracy
1.	Naïve Baiyes Algorithm	91.884
2.	Logistic Regression Algorithm	90.448
3.	K-Nearest Neighbor Algorithm	93.963
4.	Random Forest Algorithm	94.001
5.	Support Vector Machine Algorithm	94.9991

IV. CONCLUSION

This research is all about studying credit card fraud-detection models based on different machine learning classification algorithms. The goal is to be in this training and testing. To find out the best way to process the dataset and the best machine learning classification algorithm for the dataset of this credit card transaction.

So to achieve this, we chose five different classifiers, respectively. Between them, ten different combinations of algorithms and sampling methods were used to evaluate their predicted performance as a way to get better results for credit card fraud detection. Finally, we cross-validated the technique applied to all the individual classifiers to obtain more accurate results.

We also have some findings for this study:

- Using oversampling to deal with a too unbalanced credit card transaction dataset in the confusion matrix ended up with the same results as we expected.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204091 |

- Logistic regression, as one of the simpler few algorithms, still has their advantages in targeting differential data processing, followed by the SVM algorithm. There is also the catboost algorithm which both perform well
- We can compare to the previously mentioned literature for the model training and testing, this study obtains an optimal machine learning algorithm for credit card fraud detection - logistic regression (oversampling) - and also achieves high accuracy results.

REFERENCES

1. D. M. Kumar, V. K. Gunjan, M. D. Ansari, and R. Pathak, ''Credit card fraud detection using support vector machine,'' in Proc. 2nd Int. Conf. Recent Trends Mach. Learn., IoT, Smart Cities Appl. (Lecture Notes in Networks and Systems), 2022, pp. 27–37, doi: 10.1007/978-981-16-6407- 6_3.
2. N. Carneiro, G. Figueira, and M. Costa, ``A data mining-based system for credit-card frauddetection in e-tail," Decis. Support Syst., vol. 95, pp. 91101, Mar. 2017.
3. B. Lebichot, Y.-A. Le Borgne, L. He-Guelton, F. Oblé, and G. Bontempi, ``Deep-learningdomain adaptation techniques for credit cards fraud detection," in Proc. INNS Big Data Deep Learn. Conference, Genoa, Italy, 2019, pp. 7888.
4. Kleinbaum, D.G., Klein, M. (2010). Logistic Regression for Correlated Data: GEE. In: LogisticRegression. Statistics for Biology and Health. Springer, New York\.
5. Adewumi AO, Akinyelu AA (2017) A survey of machine-learning and nature-inspiredbased credit card fraud detection techniques. Int J Syst Assur Eng Manag 8(2):937–11, 28941-28961.
6. M.Seera, C. P. Lim, A. Kumar, L. Dhamotharan, and K. H. Tan, ''An intelligent payment card fraud detection system,'' Ann. Oper. Res., pp. 1–23, Jun. 2021, doi: 10.1007/s10479-021-04149-2.
7. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, ''A neural network ensemble with feature engineering for improved credit card fraud detection,'' IEEE Access, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/access.2022.3148298.
8. N. Rtayli and N. Enneya, ''Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization,'' J. Inf. Secur. Appl., vol. 55, Dec. 2020, Art. no. 102596, doi: 10.1016/j.jisa.2020.102596.
9. K. Li, N. Ding, Y. Zhai, and H. Dong, ''Comparative study on credit card fraud detection based on different support vector machines,'' Intell. Data Anal., vol. 25, no. 1, pp. 105–119, Jan. 2021, doi: 10.3233/ida-195011.
10. C. Mniai and K. Jebari. (Jul. 2022). Credit Card Fraud Detection by Improved SVDD. ResearchGate. [Online].

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com