iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50849

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

Credit Card Fraudulent Transaction Detection and Prevention

Prof. S. R. Salian[1], Dipa D. Kamble[2], Shivani R. Kotwal[3], Sandhya L. Kapal[4], Rasika B. Hiware[5]
[1]*Prof. Computer Engineering. Datta Meghe College of Engineering, Airoli - Navi Mumbai, Maharashtra*
[2, 3, 4, 5]*Students. Datta Meghe College of Engineering, Airoli - Navi Mumbai, Maharashtra*

Abstract: ***In recent years, online payment methods have been used widely as an outcome of the rapid increase in non-cash and digital electronic transactions. Credit cards represent one of the electronic payment methods. With the advancement of online payments in various products and services, the likelihood of credit card fraud has risen compared to the decades-long history of credit cards. The credit card frauds can be detected by evaluating the credit card purchasing patterns using the historical data in order to detect the frauds. This data evaluation can help the banks or other organizations offering credit cards to minimize their losses due to the credit card frauds. The historical data evaluation with the current purchasing patterns requires statistical modeling, which can automatically evaluate the fraudulent patterns and alarm the banks about the transactions. This helps the banks for early detection of the frauds, where they can easily eliminate the credit card frauds by declining the suspected transactions. And also blockchain technology is applied to prevent the hacker to view customers details so that fraudsters can't use stolen credit card information to open new accounts, obtain loans, and engage in other illegal activities.***
Credit card fraud detection and prevention have become essential for banks and other financial institutions to safeguard their customers' financial transactions. This paper presents an overview of credit card fraud detection and prevention techniques.
Keywords: Credit card, Digital electronic transaction, Fraud detection, Logistic regression algorithm and Fernet Algorithm(Blockchain).

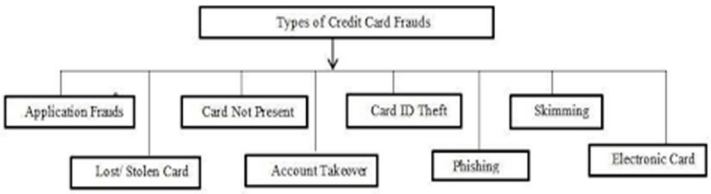
I. INTRODUCTION

E-commerce has come a long way since its inception. It has become an essential means for most organizations, companies, and government agencies to increase their productivity in global trade. One of the main reasons for the success of e-commerce is the easy online credit card transaction. Whenever we talk about monetary transactions, we also have to take financial fraud into consideration. Financial fraud is an intentional crime in which a fraudster benefits himself/herself by denying a right to a victim or by obtaining financial gain. As credit card transactions are the most common method of payment in recent years, the fraud activities have increased rapidly. There are 1.06 billion credit cards in use in America and 2.8 billion credit cards worldwide. A US citizen, on average, has four active credit cards. In the European Union (EU), the number of cards carried per person ranges from 0.8 to 3.9. The numbers have only grown since then from 2016 to now.There were 368.92 billion card transactions worldwide in 2018. However, the average value per card payment is decreasing in most of the major economies, as a credit card is used more and more as a preferred financial product compared to other means. The average value per card payment drop indicates that customers are using a credit card more and more for daily use compared to one-off events like big purchases.

There are different types of credit card fraud they are:

1) *Counterfeit Card Fraud:* This occurs when a thief creates a fake card using stolen card information.
2) *Lost or Stolen Card Fraud:* This happens when a thief steals a credit card and uses it before the owner can report it lost or stolen.
3) *Identity Theft:* This is when a thief uses stolen personal information to open a new credit card account in someone else's name.
4) *Card-not-present Fraud:* This occurs when a thief uses stolen card information to make purchases online or over the phone.
5) *Skimming:* This happens when a thief uses a device to steal credit card information from a card's magnetic stripe, typically at an ATM or gas pump.
6) *Phishing:* This is when a thief uses fraudulent emails or websites to trick people into providing their credit card information.
7) *Chargeback Fraud:* This occurs when a consumer disputes a legitimate charge, claiming it was fraudulent, in order to get their money back.

©IJRASET: All Rights are Reserved



A. Motivation

Credit card fraud is a significant problems that affect individuals, businesses and financial institutions. Fraudulent transaction can result in stolen identities, lost revenue and damage reputations. And due to Digital India schema and covid-19 period the use of online payment has been increased. So we tried to build the model that detect fraud in instant

B. Problem Statement

Credit cards are a crucial financial tool that give their owners the convenience of making purchases now and having the option to pay the balance later. Owners of credit cards benefit from deferring payment for a predetermined period of time. Because of this, credit cards are an obvious target for scammers. These scammers can withdraw a sizeable sum of money without the owner's knowledge while making it appear as though the real cardholders made the withdrawal. Because they operate covertly and with great care, that became easier for fraudsters to hack data and use customer card based on their detail to use for transaction.

C. Objectives

The primary objectives of credit card fraud detection and prevention using ML and blockchain are:

1) To minimize losses due to credit card fraud.
2) To improve the efficiency of fraud detection and prevention.
3) To provide a secure and reliable payment system for customers.
4) To enhance customer trust and confidence in financial institutions.
5) To comply with regulatory requirements and industry standards.

By achieving these objectives, financial institutions can ensure that credit card transactions are secure, efficient, and trustworthy, providing peace of mind to customers and businesses alike.

II. LITERATURE REVIEW

1) Kuldeep Randhawa et al. [10] proposed supervised machine learning algorithms on realworld data and then used these algorithm s to use superclassification using hash learning, and then compared the performance of the tracking algorithm with the use of sup erclassifiers. They use several machine learning algorithms such as Isolation Forest, Local Outlier Value Factor, and Logistic Re gression. They then compare the true, true inverse, confusion matrix with the results of their superclassifier. As a result, they fou nd that logistic regression was better at predicting job fraud.

2) John O. Awoyemi et al. [14] proposed a model based on ANN and metavalue method to optimize risk and loss. Neural network t echniques for credit card fraud prevention and detection. Fraud can be difficult to detect due to the disparity of information (frau d and nonfraud).Added meta value method to fix issues with unstable data. Cost Sensitive Neural Networks (CSNN) are based o n torture detection. The model offers cost savings and growth compared to the Artificial Immune System (AIS). This survey data comes from major credit card companies in Brazil who provide realtime transaction data.

3) Abhimanyu Roy et al.[11] reported a deep learning method for fraud detection in online money transactions. This approach is pr ovided by nonstandard electronic devices with shortterm memory and a few other physical and memorydevices. Based on the eff ectiveness of these products in detecting fraud, approximately 80 million online credit card transactions have been found to be fr audulent and legitimate. They use the best performance in cloud computing environment. The study presented by the researchers offers good advice for conducting a sensitivity analysis of restrictions on fraud studies.Researchers are also preparing a framewo rk for deep learning topology parameter tuning for fraud. This allows financial institutions to save money by avoiding fraud.

4) Rimpal R. Popat and Jayesh Chaudhary present a survey evaluating the performance of various algorithms when applied to multi problem loan data. 284,807
algorithm machine for European cards.However, none of these studies consider the use of multiple algorithms for post neural network datasets. Also, previous credit card fraud detection methods were not integrated with the current fraud industry.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

5) Zahra Kazemi et al. [13] proposes a method that plays a new role in this field and prevents fraud with different methods. It has b een proven to be accurate in detecting fraudulent transactions and reducing the number of false alarms.However, it comes with di stribution issues and negative price differentials

6) A. O. Adewumi and A.A. Akınyelu offers effective strategies to improve the detection of credit card fraud techniques. This resea rch focuses specifically on results based on current machine learning in the field and the credit card fraud techniques presented in this article. The survey shows the current situation in credit card verification. The scam machines now used by merchants and ba nks are designed to verify transactions by analyzing design and operation.Here, the two main methods for dealing with fraud incl ude: fraud prevention and fraud detection. The purpose of fraud prevention is to prevent fraud from occurring. The fraud detectio n strategy identifies fraudulent transactions and then defines the authorization of transactions. Machine learning is the ability to r un a computer standalone, that is, without following commands. They planned a credit card scam as a collection.This research pr ocess revealed that different machine learning algorithms are used to solve credit card fraud. Researchers need an objective meas urement system to control the distribution ofactivities with negative variable costs. Therefore, this approach can improve the perf ormance of credit card tracking mechanisms.

III. DESIGN AND IMPLEMENTATION

A. Dataset

This is a simulated credit card account with crime and fraud from January 1**,** 2019 to December 31**,** 2020. Includes credit cards of 1, 000 people. Use the market with 800 member businesses**.**

Fake source

This was created using the Sparkov Data Generating Github tool by Brandon Harris. The simulation ran from January 1**,** 2019 to De cember 31**,** 2020.

These files are combined and converted to a standard format

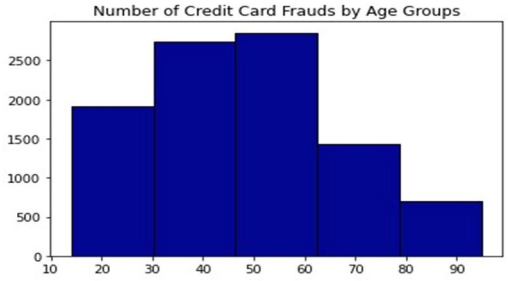
Unnamed: 0	trans_date_trans_time	cc_num	merchant	category	amt	first	last	gender	street	...	lat	long	city_pop
0	2020-06-21 12:14:25	2291163933867244	fraud_Kirlin and Sons	personal_care	2.86	Jeff	Elliott	M	351 Darlene Green	...	33.9659	-80.9355	333497
1	2020-06-21 12:14:33	3573030041201292	fraud_Sporer-Keebler	personal_care	29.84	Joanne	Williams	F	3638 Marsh Union	...	40.3207	-110.4360	302
2	2020-06-21 12:14:53	3598215285024754	fraud_Swaniawski, Nitzsche and Welch	health_fitness	41.28	Ashley	Lopez	F	9333 Valentine Point	...	40.6729	-73.5365	34496
3	2020-06-21 12:15:15	3591919803438423	fraud_Haley Group	misc_pos	60.05	Brian	Williams	M	32941 Krystal Mill Apt. 552	...	28.5697	-80.8191	54767
4	2020-06-21 12:15:17	3526826139003047	fraud_Johnston-Casper	travel	3.19	Nathan	Massey	M	5783 Evan Roads Apt. 465	...	44.2529	-85.0170	1126

job	dob	trans_num	unix_time	merch_lat	merch_long	is_fraud
Mechanical engineer	1968-03-19	2da90c7d74bd46a0caf3777415b3ebd3	1.371817e+09	33.986391	-81.200714	0.0
Sales professional, IT	1990-01-17	324cc204407e99f51b0d6ca0055005e7	1.371817e+09	39.450498	-109.960431	0.0
Librarian, public	1970-10-21	c81755dbbbea9d5c77f094348a7579be	1.371817e+09	40.495810	-74.196111	0.0
Set designer	1967-07-25	2159175b9efe66dc301f149d3d5abf8c	1.371817e+09	28.812398	-80.883061	0.0
Furniture designer	1955-07-06	57ff021bd3f328f8738bb535c302a31b	1.371817e+09	44.959148	-85.884734	0.0

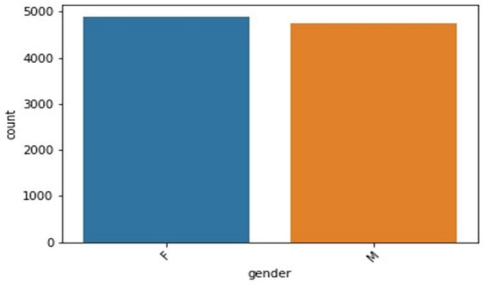
B. Implementation

1) Import required libraries like pandas, numpy, sklearn, matplotlib, seaborn.
2) Use pandas to upload files.
3) Process data by removing missing values, duplicates, and outliers.
4) Custom selection using correlation analysis and significance analysis.
5) Distribute data for training and testing.
6) Use training methods to train logistic regression models.
7) Optimizing models without using techniques such as competition.
8) Evaluate the performance of the model using metrics such as accuracy, precision, recall, and F1 score.
9) Visualize the results using matplotlib and seaborn.
10) Use patterns to detect fraudulent transactions in real time**.**
11) Finally**,** we secured the customer database using the blockchain algorithm, which is the Fernet algorithm.

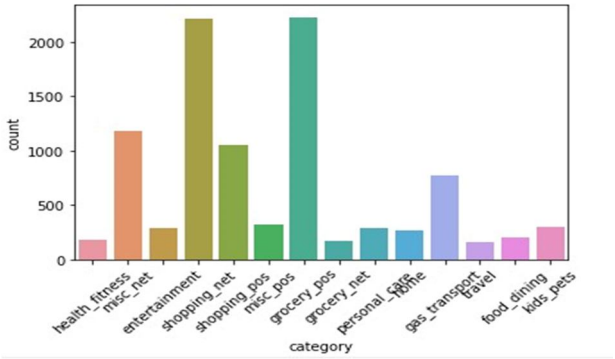
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



Here we can observe from the histogram that Age group of 50-60 had commited more crime.

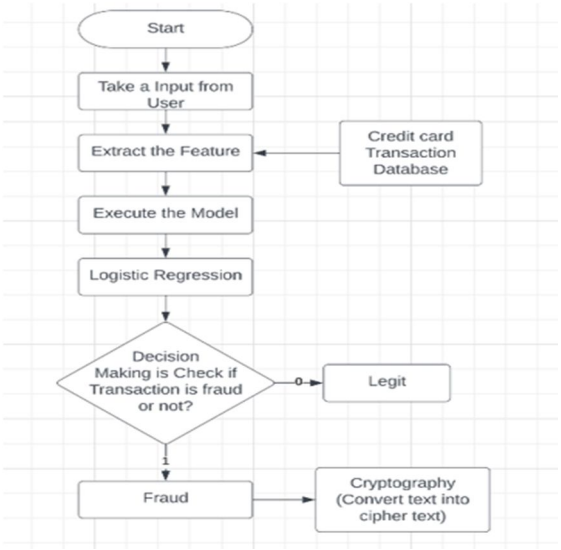


Here we can observe which gender types the credit card fraud has occurred more.

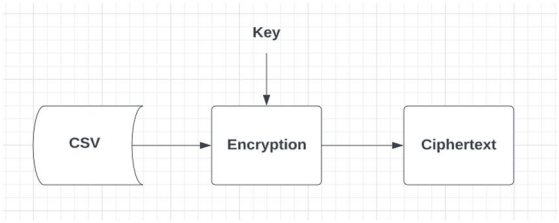


Here we can observe from the bar graph the category of merchant that uses credit card more.

C. Flowchart



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com



D. Model Used

1) Detection Method

Machine Learning

2) Logistic Regression

Logistic regression is a statistical model that is commonly used in machine learning for classification problems. In the context of credit card fraud detection, logistic regression can be used to classify credit card transactions as either fraudulent or legitimate based on various features such as transaction amount, location, time of day, etc.

The logistic regression model works by fitting a logistic curve to the input data, which is a type of sigmoidal function that ranges from 0 to 1. The logistic curve is used to model the probability of an event occurring, in this case, the probability that a credit card transaction is fraudulent.

During training, the logistic regression model learns the optimal parameters that maximize the likelihood of the observed data given the model. These parameters are then used to make predictions on new data by feeding the input features through the logistic curve to obtain a predicted probability of fraud.

If the predicted probability of fraud is above a certain threshold, the transaction is classified as fraudulent, otherwise, it is classified as legitimate. The threshold can be adjusted based on the specific requirements of the credit card company, such as the tradeoff between false positives and false negatives.

Logistic regression is a popular choice for credit card fraud detection because it is a simple yet effective model that can provide interpretable results. However, it may not perform well in more complex scenarios where the relationship between the input features and the target variable is non-linear. In these cases, more advanced machine learning models such as neural networks may be used.

3) Prevention Method

Blockchain Technology

4) Fernet Algorithm

Fernet is a cryptographic library in Python that provides security. It is commonly used for encrypting and decrypting data. Fernet uses symmetric encryption, which means that it uses the same key for both encryption and decryption. Without the key hacker can't decrypt the sensitive data and the key only the authorized person only know. In the context of credit card fraud prevention, Fernet can be used to encrypt sensitive data such as credit card numbers, addresses and names. This can help prevent data breaches and protect customer information.

Overall, Fernet is a valuable tool for credit card fraud prevention as it provides a high level of security for sensitive data.

IV. RESULT AND DISCUSSION

We have obtained the accuracy of 94.62% which is obtained using logistic regression in credit card fraud detection model. It means that the model is able to correctly classify 94.62% of the credit card transaction as either fraudulent or legimate. Along with it we have provided confusion metrics.

```
confusion matrix
[[ 15489  21807]
 [     0 368451]]
accuracy score:
0.9462546858017434

precision score:
0.993826977376371
```

©IJRASET: All Rights are Reserved

V. CONCLUSION

As a result, the combination of machine learning (ML) and blockchain technology can be a powerful tool for detecting and preventi ng credit card fraud. Machine learning algorithms can analyze large volumes of transaction data to identify fraudulent patterns and a nomalies**.** Blockchain, on the other hand, offers a secure and tamperproof way to store and distribute this information, making it harder for scammers to manipulate or change the information.Credit card companies can improve fraud and p revention capabilities, potentially reduce financial losses, and improve customer service by using machine learning to identify poten tial fraud and blockchain to protect sensitive data**.** However, it is important to remember that this transaction **is** not fraudulent and ad ditionl security measures must be taken to ensure that the card withdrawal **is** fully protected.

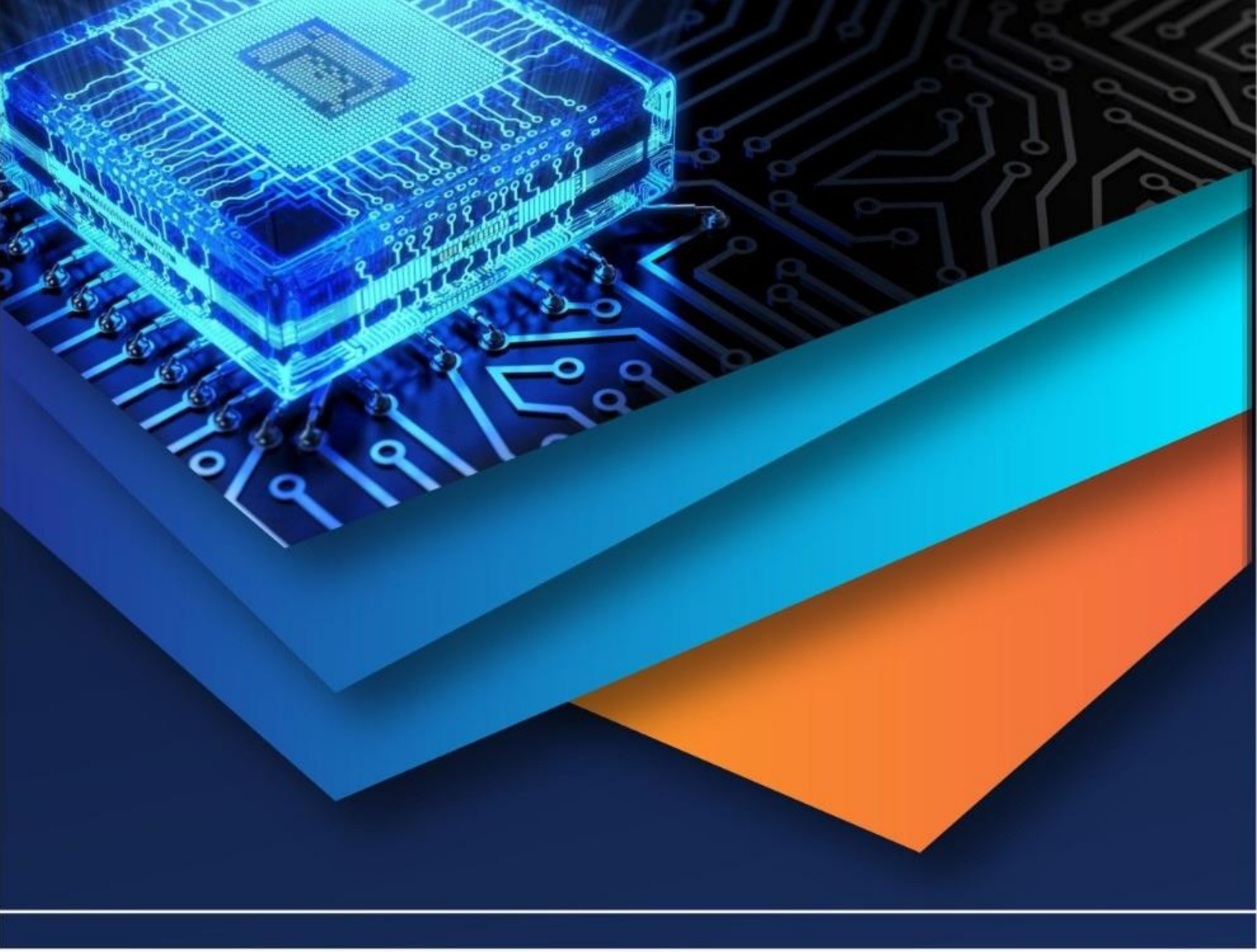
VI. FUTURE SCOPE

1) Multi-factor authentication: Machine Learning models could be integrated with other security measures, such as multi-factor authentication, to provide an additional layer of protection against fraud.
2) Unsupervised learning: Current fraud detection systems use supervised learning techniques that require labeled data. However, unsupervised learning techniques could be developed to identify patterns and anomalies in transaction data without the need for labeled data
3) Cross-border transactions: Machine Learning and blockchain can also facilitate cross-border transactions by enabling quick and secure verification of international transactions. This can help reduce fraud and improve the efficiency of global payments.
4) Smartcontract-based fraud detection: Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, can be used to automate fraud detection. By incorporating machine learning algorithms into smart contracts, fraud detection can be automated and streamlined, reducing the need for human intervention.

REFERENCES

[1] Fraud Detection Using Machine Learning: https://aws.amazon.com/ru/solutions/fraud-detection-using-machine-learning/
[2] Credit Card Fraud Detection using Machine Learning Algorithms https://www.sciencedirect.com/science/article/pii/S187705092030065X
[3] ML | Credit Card Fraud Detection: https://www.geeksforgeeks.org/ml-credit-card-fraud-detection/
[4] Detecting Credit Card Fraud using Machine Learning: https://www.researchgate.net/publication/357213297_Detecting_Credit_Card_Fraud_using_Machine_Learning
[5] Credit Card Fraud Detection: https://www.ijraset.com/research-paper/credit-card-fraud-detection
[6] Credit Card Fraud Detection using Deep Learning: https://ieeexplore.ieee.org/document/9033906
[7] Credit Card Fraud Prevention Using Blockchain: https://ieeexplore.ieee.org/document/9418192
[8] S.B.E. and Portia, A.A., Raj, "Analysis on credit card fraud detection methods, "International Conference on Computer, Communication and Electrical Technology (ICCET): https://ieeexplore.ieee.org/document/5762457
[9] A New Method for Fraud Detection in Credit Cards Based on Transaction Dynamics in Subspaces: https://doi.org/10.1109/CSCI49370.2019.00137
[10] Using deep networks for fraud detection in the credit card transactions: https://doi.org/10.1109/KBEI.2017.8
[11] Dataset: https://www.kaggle.com/code/ambarishdeb/credit-card-fraud-prediction-eda-ml-evaluation

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)