iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41704

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 10 Issue IV Apr 2022- Available at www.ijraset.com

Credit Card Fraud Detection project

Rashi Saini[1], Prof. Bipin Pandey[2]
[1]*Student,* [2]*Professor & HOD, Computer Science Engineering, Dronacharya Group of Institutions, Greater Noida, UP, India*

Abstract: ***For some time, there has been a strong interest in the ethics of banking (Molyneaux, 2007; George, 1992), as well as the moral complexity of fraudulent behavior (Clarke, 1994). Fraud means obtaining services/goods and/or money by unethical means, and is a growing problem all over the world nowadays. Fraud deals with cases involving criminal purposes that, mostly, are difficult to identify. Credit cards are one of the most famous targets of fraud but not the only one; fraud can occur with any type of credit products, such as personal loans, home loans, and retail. Furthermore, the face of fraud has changed dramatically during the last few decades as technologies have changed and developed. A critical task to help businesses and financial institutions including banks is to take steps to prevent fraud and to deal with it efficiently and effectively, when it does happen (Anderson, 2007). Anderson (2007) has identified and explained the different types of fraud, which are as many and varied as the financial institution's products and technologies, such as Transaction products: credit and debit cards and checks, Relationship to accounts first, second and third parties, Business processes: application and transaction, Manner and timing short versus long term, Identify misrepresentation: embellishment, theft and fabrication, Handling of transaction: lost or stolen, not received, skimming and at hand, Utilization counterfeit, not present, altered or unaltered, Technologies ATM and Internet.***
Solutions for integrating sequential information in the feature set exist in the literature. The predominant one consists in creating a set of features which are descriptive statistics obtained by aggregating the sequences of transactions of the card-holders (sum of amount, count of transactions, location from where the payment is being made etc..). We used this method as a benchmark feature engineering method for credit card fraud detection. However, this feature engineering strategy raised several research questions. First of all, we assumed that these descriptive statistics cannot fully describe the sequential properties of fraud and genuine patterns and that modelling the sequences of transactions could be beneficial for fraud detection. Moreover, the creation of these aggregated features is guided by expert knowledge whereas sequence modelling could be automated thanks to the class labels available for past transactions. Finally, the aggregated features are point estimates that may be complemented by a multi-perspective univariate description of the transaction context. We proposed a multi-perspective HMM-based automated feature engineering strategy in order to incorporate a broad spectrum of sequential information in the transactions feature sets. In fact, we model the genuine and fraudulent behaviors of the merchants and the card-holders according to two univariate features: the country from where the payment is being made and the amount of each of the transactions being made. Moreover, the HMMbased features are created in a supervised way and therefore lower the need of expert knowledge for the creation of the fraud detection system. In the end, our multiple perspectives HMM-based approach offers automated feature engineering to model temporal correlations so as to complement and possibly supplement the use of transaction aggregation strategies in order to improve the effectiveness of the classification task. Experiments conducted on a large real world credit card transaction dataset (46 million transactions from belgium card-holders between March and May 2015) have shown that the proposed HMM-based feature engineering allows for an increase in the detection of fraudulent transactions when combined with the state-of-the-art expert-based feature engineering strategy for credit card fraud detection. To conclude, this work leads to a better understanding of what can be considered contextual knowledge for a credit card fraud detection task and how to include it in the classification task in order to get an increase in fraud detection. The method proposed can be extended to any supervised task with sequential datasets. The main aims are, firstly, to identify the different types of credit card fraud, and, secondly, to review alternative techniques that have been used in fraud detection. Indeed, transaction products, including credit cards, are the most vulnerable to fraud. On the other hand, other products such as personal loans and retail are also at risk, and have serious ethical conflicts.

Keywords: Behavior and Location Analysis (BLA); Fraud Detection System (FDS); Automated Teller Machine (ATM); Credit Card Fraud Detection; DB: Database.

I. INTRODUCTION

Nowadays Credit card usage has drastically increased across the world, now people believe in going cashless and are completely dependent on online transactions. The credit card has made the digital transaction easier and more accessible. A huge number of dollars of loss are caused every year by criminal credit card transactions. Fraud is as old as mankind itself and can take an unlimited variety of different forms.

The PwC global economic crime survey of 2017 suggests that approximately 48% of organizations experienced economic crime. Therefore, there's positively a necessity to unravel the matter of credit card fraud detection. Moreover, the growth of new technologies provides supplementary ways in which criminals may commit a scam. The use of credit cards is predominant in modern day society and credit card fraud has been kept on increasing in recent years. Huge Financial losses have been fraudulent effects on not only merchants and banks but also the individual person who are using the credits. Fraud may also affect the reputation and image of a merchant causing non-financial losses that. For example, if a cardholder is a victim of fraud with a certain company, he may no longer trust their business and choose a competitor. Fraud Detection is the process of monitoring the transaction behavior of a cardholder to detect whether an incoming transaction is authentic and authorized or not otherwise it will be detected as illicit.

Credit card fraud is a huge ranging term for theft and fraud committed using or involving at the time of payment by using this card. The purpose may be to purchase goods without paying, or to transfer unauthorized funds from an account. Credit card fraud is also an add on to identity theft. As per the information from the United States Federal Trade Commission, the theft rate of identity had been holding stable during the mid 2000s, but it was increased by 21 percent in 2008. Even though credit card fraud, that crime which most people associate with ID theft, decreased as a percentage of all ID theft complaints in 2000, out of 13 billion transactions made annually, approximately 10 million or one out of every 1300 transactions turned out to be fraudulent. Also, 0.05% (5 out of every 10,000) of all monthly active accounts was fraudulent. Today, fraud detection systems are introduced to control one-twelfth of one percent of all transactions processed which still translates into billions of dollars in losses. Credit Card Fraud is one of the biggest threats to business establishments today. However, to combat fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card fraudsters employ a large number of ways to commit fraud. In simple terms, Credit Card Fraud is defined as "when an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used". Card fraud begins either with the theft of the physical card or with the important data associated with the account, including the card account number or other information that necessarily be available to a merchant during a permissible transaction. Card numbers, generally the Primary Account Number (PAN) are often reprinted on the card, and a magnetic stripe on the back contains the data in machine-readable format. It contains the following Fields: Name of card holder, Card number, Expiration date, Verification/CVV code, Type of card. There are more methods to commit credit card fraud. Fraudsters are very talented and fast-moving people. In the Traditional approach, to be identified by this paper is Application Fraud, where a person will give the wrong information about himself to get a credit card. There is also the unauthorized use of Lost and Stolen Cards, which makes up a significant area of credit card fraud. There are more enlightened credit card fraudsters, starting with those who produce Fake and Doctored Cards; there are also those who use Skimming to commit fraud. They will get this information held on either the magnetic strip on the back of the credit card, or the data stored on the smart chip is copied from one card to another. Site Cloning and False Merchant Sites on the Internet are becoming a popular method of fraud for many criminals with a skilled ability for hacking. Such sites are developed to get people to hand over their credit card details without knowing they have been swindled.

To deal with such type of Credit Card Frauds, in the proposed system, I present a behavior and Location Analysis (BLA). Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. Card transaction processing sequence by the stochastic process of a BLA. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Hence, I feel that BLA is an ideal choice for addressing this problem. Another important advantage of the BLA - based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

The credit card fraud detection features use user behavior and location scanning to check for unusual patterns. These patterns include user characteristics such as user spending patterns as well as usual user geographic locations to verify his identity. If any unusual pattern is detected, the system requires re-verification. The system analyses user credit card data for various characteristics. These characteristics include user country, usual spending procedures. Based upon previous data of that user the system recognizes unusual patterns in the payment procedure. So now the system may require the user to login again or even block the user for more than 3 invalid attempts.

The Modules and their Description: This system has 6 Modules: Registration, Login, Payment, Verification, Feedback, Logout.

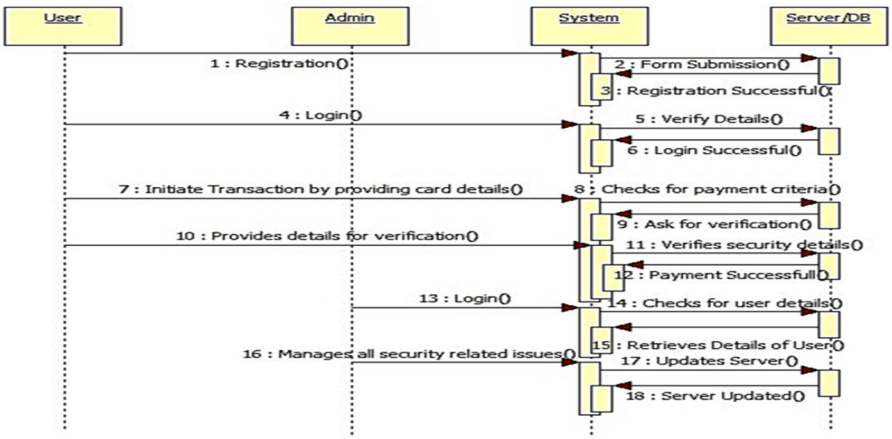
A. Description

1) *Step 1:* Registration: Here, users first need to register themselves with their respective details to access the system.
2) *Step 2:* Login: After a successful registration, users then need to login into the system by inputting their credentials into the system.
3) *Step 3:* Payment: Users can select payment mode to perform transactions by providing card details like card no., CVV code, Expiry Date and Holders name.
4) *Step 4:* Verification: If the user performs a huge transaction, then for security purposes, the system will automatically redirect to the verification page to verify the user and to prevent misuse of card in case lost.
5) *Step 5:* Feedback: Here, the user may provide feedback to the admin regarding the working of the system.
6) *Step 6:* Logout: After a successful transaction, users may log out from the system.

Our Paper is organized as follows: Methodology is presented in section II. Procedure Used is presented in section III. Finally, the result and Conclusions are presented in sections IV and V respectively.

II. METHODOLOGY

We have four basic modules in the given system named as User, Admin, System, Server/DB shown in the figure below which perform their respective operations:



1) *Step 1:* User performs the registration of him/her self to the system such that system performs the form submission function (send details to the database) and Server/DB provides the response that registration is being done successfully to the System after all the details have been successfully stored in the database.
2) *Step 2:* Then user performs the Login operation to the System which in turn performs the VerifyDetails function, verifies the details entered by the user to the system from the details of the respective user stored in the database. If the details of the user match with his/her details stored in the database, then server allows the user to access the system.
3) *Step 3:* User initiates the transaction by providing card details to the system which in turn passes the command to the Server/DB to check for the payment criteria.
4) *Step 4:* If there is any detail found stored in the database which does not match with the details provided by the user to the Server/DB then database redirects user for verification.
5) *Step 5:* User then provides the details required by database for verification to the system which in turn provides those details to the database to verify the security details entered by the user against the details of user stored in database.
6) *Step 6:* If the security details provided by the user match with the security details stored in the database of the respective user, then the transaction made by the user becomes successful.
7) *Step 7:* Admin performs Login operation to the System to modify/Delete/access for any user details, Server/DB retrieves details of the user to the system and user successfully get logged in.
8) *Step 8:* Admin also Manages all the security related issues to the System which further get updated to the server and after server gets updated it acknowledges the same to the System.

The following Project Implementation Technology is used in the project:
The Project is loaded in Visual Studio 2010. We used Visual Studio for Design and coding of the project. Created and maintained all databases into SQL Server 2008, in that we create tables, write queries for store data or record of project. Hardware Requirement: - i3 Processor Based Computer, 1GB-Ram, 5 GB Hard Disk. Software Requirement: Windows XP, Windows 7(ultimate & enterprise), Visual studio 2010, SQL Server 2008.
Users perform various tasks such as Registration, Login, Payment, Update Details, Checks Details, Verification, Provides Feedback on the system. User and Administrator are connected to each other via system. System is the interconnecting link present which connects Users to the Administrator and vice-versa. The administrator handles tasks such as Registration, Login, Update Details, Checks Details provided by the user to the system, and also it manages all the security related issues.

III. PROCEDURE USED

Credit card fraud detection project is an advanced system that consists of various algorithms inside it to detect credit card fraud suppose someone knows the details of the user and he is using the credit card so the system has inbuilt algorithms to detect and check the validity of the user who is making the payment through this card so first of all the basic requirement would be to check the details as a normal payment gateway does so it first checks the details were whether the name on the card is right, the card number, CVV code, date of expiry, all the details and after that it also checks the user's spending pattern so suppose if the user usually makes payments of 50 to 100 and one day he makes a payment of around 150 or 250 which is not his usual spending pattern so system doesn't directly allow the payment even if all the credit card details are right it takes the user to the security page to ask him security questions to check validity of the user and one more monitoring feature of Credit Card Fraud Detection System is the user country, many credit card frauds happen from stolen credit card details and people from other countries make the payment from those countries which even if get detected are not easy to identify, it also detects the country through IP address so, if it detects that user has usually made successful payments from two to three countries or whichever countries he has made payments in the last payment patterns, from his last recorded data it checks the user country and if user deviates from that pattern and gets a payment from some other country so, it again takes the user to the verification page where it asks some security questions which only the user would know and if he enters those questions right only then system allows the payment or else it stops the payment and blocks the account. Suppose there is any new user so the user should register first as we already have a username password so if the user enters the wrong details the name, CVV number, credit card number so system is going to stop him so he must enter the right details as when we use the system for a start our data is empty, the data for our spending patterns is not there in the system so for first 10 transactions the system is going to allow us to make the transaction it can't stop us because it doesn't have our spending pattern so once it gets 10 transactions it will start monitoring our transactions after that as we have already made some transactions in the system which are more than 10 so those amounts of transactions are locked through the system itself so, if they are in the five thousand to eight thousand range so we can take an average of about six thousand to seven thousand if we try entering an amount a little bit greater than the average amount so the system takes an approximation average of the current values entered by the user in the hispanic pattern and then it sees if the current transaction value deviates more than thirty percent or forty percent than his normal spending pattern if it is found it takes user to the security page If user enters twenty thousand and click on pay it doesn't allow the payment it asks the user security questions so, if we get back to the page and enter 5000 that is within the range and we enter some other country from which the user hasn't yet operated yet so besides from India, China, USA if we'll enter some other country and click on pay so it asks the security question again if we go back. So, one more feature we have in our system is if user spends around deviates around 20 than his average spending pattern but he is still from the operating from the same country so he can make transactions his transaction amount can deviate more than 30 to 40 percent from his normal spending pattern since he is from the operating from the same country if he is operating from a different country the system allows the user for a successful transaction only if the amount deviates more than 20 or around 20 percent, if the situation gets reversed amount deviates more than 20 and he is operating from a country which is not in his list from which he has never operated before it stops the user again so this is how credit card fraud detection system works.

IV. RESULT AND DISCUSSIONS

We have used the Behavior and Location Analysis approach to identify any Credit Card Fraud. It uses user behavior and location scanning to check for unusual patterns. These patterns include user characteristics such as user spending patterns as well as usual geographic locations to verify his identity. If any unusual pattern is detected, the system requires re-verification.The system analyses user credit card data for various characteristics.

These characteristics include country, usual spending procedures. Based upon previous data of that user the system recognizes unusual patterns in the payment procedure. So now the system may require the user to login again oz even block the user for more than three invalid attempts.

Even though there are many fraud detection techniques we can't say that this particular BLA based algorithm detects the fraud completely. From our analysis, we can conclude that the accuracy of BLA algorithm is really good. It is evident from the above review that several machine learning algorithms are used to detect fraud, but the findings are not satisfactory. As a result, we'd like to use BLA based algorithms to reliably detect credit card fraud. Our Project main purpose is to making Credit Card Fraud Detection awaking to people from credit card online frauds. The main point of the credit card fraud detection system is necessary to save our transactions & security. Our aim here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications.

Our project is technically feasible because all the technology needed for our project is readily available.

Operating System : Windows XP, 7(ultimate & enterprise)
Languages : Asp.Net with C# (.Net 2010)
Database System : MS-SQL Server 2008
Documentation Tool : MS - Word 2013

Our project is economically feasible because the cost of development is very minimal when compared to the financial benefits of the application, also our project is operationally feasible because the time requirements and personnel requirements are satisfied. I have worked on this project by myself as I am the only team member of the project team, and I worked on this project for five working months. The system stores previous transaction patterns for each user, based upon the user spending ability and even country, it calculates user's characteristics, more than 20 -30 % deviation of user's transaction (spending history and operating country) is considered as an invalid attempt and system takes action. As the project is on a bit large scale, we always need testing to make it successful. If each component works properly in all respects and gives the desired output for all kinds of inputs then the project is said to be successful. So, the conclusion is to make the project successful, it needs to be tested. The testing done here was System Testing checking whether the user requirements were satisfied. The code for the new system has been written completely using ASP .NET with C# as the coding language, C# as the interface for front-end designing. The new system has been tested well with the help of the users and all the applications have been verified from every nook and corner of the user. Our System is: Load Balancing: since the system will be available only the admin logs in the amount of load on server will be limited to time period of admin access, Easy Accessibility: Records can be easily accessed and stored and other information respectively, User Friendly: The system will be giving a very user-friendly approach for all users, Efficient and reliable: Maintaining the all secured and database on the server which will be accessible according the user requirement without any maintenance cost will be a very efficient as compared to storing all the customer data on the spreadsheet or physically in the record books, Easy maintenance: Credit Card Fraud Detection System is designed as easy way. So, maintenance is also easy.

V. CONCLUSIONS

Clearly, credit card fraud is an act of criminal dishonesty. This article has reviewed recent findings in the credit card field. This paper has identified different types of fraud, such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud, and discussed measures to detect them. Such measures have included pair-wise matching, decision trees, clustering techniques, neural networks, and genetic algorithms. From an ethical perspective, it can be argued that banks and credit card companies should attempt to detect all fraudulent cases. Yet, the unprofessional fraudster is unlikely to operate on the scale of the professional fraudster and so the costs to the bank of their detection may be uneconomic. The bank would then be faced with an ethical dilemma. Should they try to detect such fraudulent cases or should they act in shareholder interests and avoid uneconomic costs?

A. Future Work

As the next step in this research program, the focus will be upon the implementation of a 'suspicious' scorecard on a real data-set and its evaluation. The main tasks will be to build scoring models to predict fraudulent behavior, taking into account the fields of behavior that relate to the different types of credit card fraud identified in this paper, and to evaluate the associated ethical implications. The plan is to take one of the European countries, probably Germany, and then to extend the research to other countries.

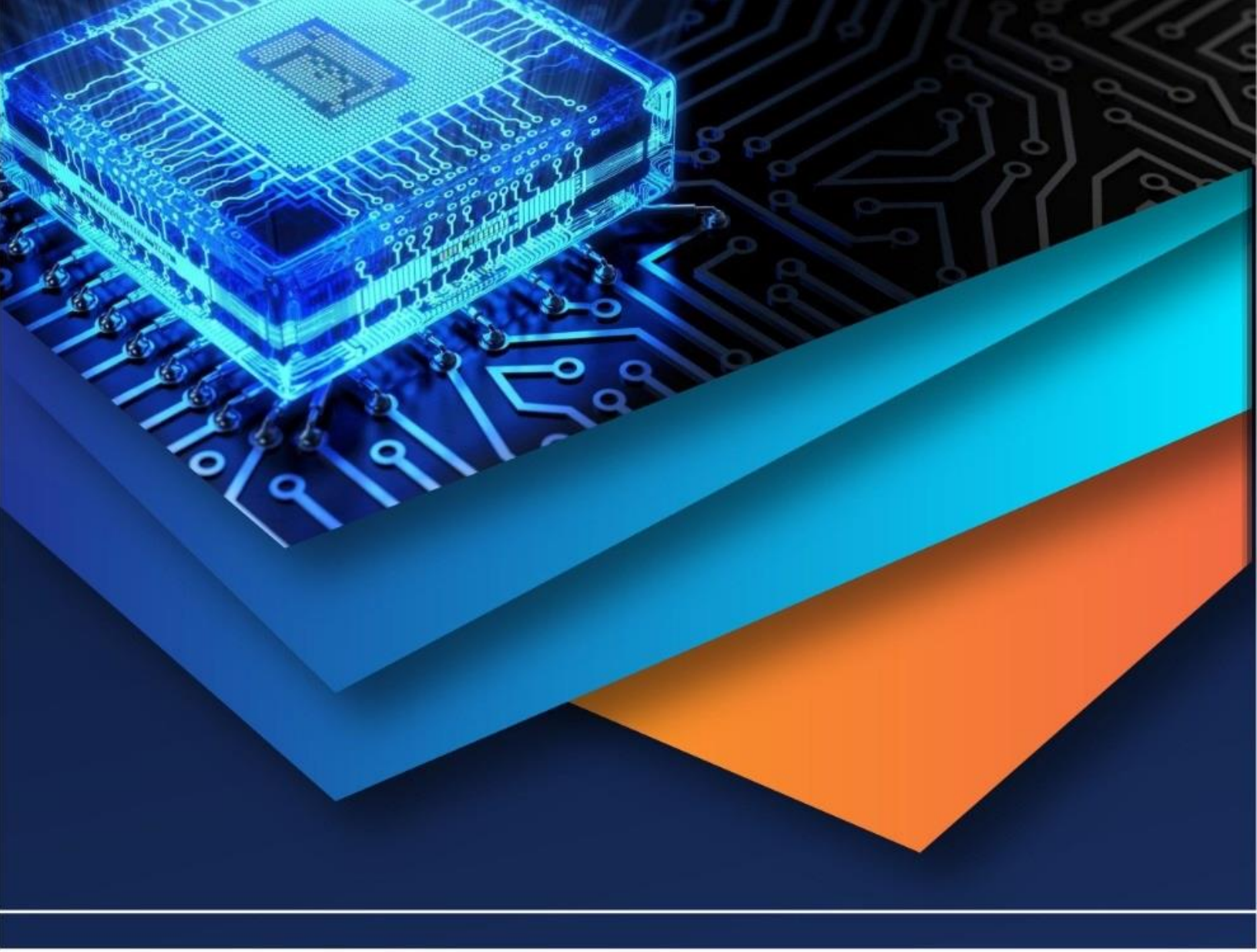
REFERENCES

[1] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5159014&queryText%3DCredit+Card+Fraud+Detection
[2] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=323314&queryText%3DCredit+Card+Fraud+Detection
[3] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5762457&queryText%3DCredit+Card+Fraud+Detection

AUTHORS

Rashi Saini is currently pursuing B.Tech in Computer Science and Engineering from Dr. APJ Abdul Kalam University, Lucknow (Uttar Pradesh). She has a wide knowledge of Java Programming, Database Management Systems, Cyber Security, Information Security, Encryption and C# language.

Bipin Pandey received the B.Tech in Computer Science & Engineering from Gautam Budha Techincal University, Lucknow (UP) and M.Tech in Computer Science and Engineering from Jodhpur National University, Jodhpur (Rajasthan). He has wide knowledge of Java Programming and Database Management Systems and Internet Programming. He is also an Oracle Certified Java Professional (OCJP) Certified professional. Currently he is leading students as HEAD OF DEPARTMENT of in Computer Science & Engineering at Dronacharya Group of Institutions, Greater Noida (Uttar Pradesh).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY