CREDIT CARD FRAUD DECTECTION USING ARTIFICAL NEURAL NETWORK

Rakibul Hoque Choudhury
Department of computer science& application,
School of Engineering & technology
Sharda University, Greater Noida,
Uttar Pradesh, India
2022611047.rakibul@pg.sharda.ac.in

Majid Iftikhar
Department of computer science & application,
School of Engineering & technology
Sharda University, Greater Noida,
Uttar Pradesh, India
2022612006.majid@pg.sharda.ac.in

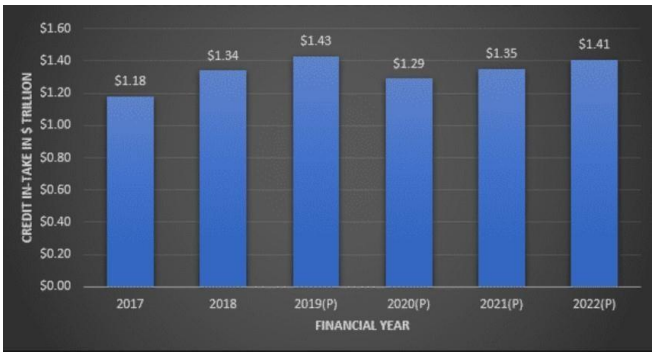
Tamisha Rani
Department of computer science & application,
School of Engineering & technology
Sharda University, Greater Noida,
Uttar Pradesh, India
2022397389.tamisha@pg.sharda.ac.in

Abstract—Online banking fraud occurs when a criminal manages to access a person's online bank account and withdraw money from it. Finding as many fraudsters as possible while reducing the amount of false alerts triggered is necessary to effectively halt this. Fraud detection and prevention are being accomplished through the use of machine learning on a larger scale. Lastly, we've offered a solution: using graphic analysis to spot fraudulent activity. It's been observed to be an effective means of ensuring confidentiality and boosting accuracy. In order to identify fraudulent transactions, credit card fraud detection frequently uses graphs, charts, and other visual data in conjunction with graphics analysis. This method uses data visualization to find anomalies and erratic patterns in credit card usage.

I. INTRODUCTION

The twenty-first century has seen a gradual opening of business facilities by the majority of financial institutions to the public through internet banking. In the competitive financial world of today, e-payment methods are imperative. Purchases of products and services are now much more convenient thanks to them. Banks often provide their customers with cards that eliminate the need for cash, making shopping simpler. By protecting purchases from possible loss, theft, or damage, credit cards provide customers with further advantages over debit cards. Customers must check with the store that the transaction is valid before completing any credit card purchase. Although credit cards offer several benefits to their users, there are also associate disks, such as fraud and security vulnerabilities. the card via dubious online sources. Anyone involved in the process, from the person whose confidential data has been leaked to the businesses (usually banks) who issue the credit card to the merchant who is completing the transaction with purchase, suffers when a fraudster compromises a person's credit or debit card. Because of this, it's critical to spot fraudulent transactions right away. Online studies state that one of the main reasons for financial losses in the banking sector is fraudulent activity related to credit and debit cards. The development of technology poses a serious risk that could cause enormous financial losses on a worldwide scale. Therefore, it is necessary to identify credit card theft in order to reduce financial losses. The era when the world was under lockdown and travel was only allowed in the most dire circumstances introduced millions of people to the world of online shopping. The past sales numbers of e-commerce platforms may be attributed, in part, to the simplicity of online buying. That there was a noticeable increase in the frequency of online financial fraud at that time should not be shocking. During the COVID-19 epidemic in 2020, there was a striking 200 percent rise in credit and debit card online fraud instances as compared to 2019.The Reserve Bank of India (RBI) provided the following figures in response to an RTI: In India, there have been 229 bank frauds on average per day in recent times, totaling transactions worth Rs.

1.38 lakh corer that have been stolen. The recovery rate for the same has been much less amazing. The process of automatically distinguishing between legitimate and fraudulent users is known as credit card fraud detection.



II. RBI is the source.

III. Numerous research projects have been carried out in arrange of fields, including as quick bone diagnostics, biometric identification, diabetes prediction, happiness prediction, and accident Avoidance at Heathrow Airport. illnesses associated with human-centered intelligent systems that prediction formational efficiency using deep neural networks. Despite these challenges, researchers continue to strive for greater accuracy in fraud detection.

IV. MOTIVATION

Graphics analysis-based credit card fraud detection is less common than more well-known transaction- based methods, but it may offer useful data and

Ideas for improving fraud protection. Several motives underlie this unusual shapes, patterns, or symbols in the actual credit card design. Even though fraud steers could attempt to mimic authentic cards, visual analysis might be able to detect subtle changes. Identifying Counterfeit Cards: To create counterfeit cards, criminals usually mimic the look of real credit cards. Graphics analysis can be used to find counter feit cards with erroneous holograms, logos, or other graphical elements.

Identifying Skimming Devices: Credit card skimming devices, for instance, are used to steal card information from real card sat ATM sand petrol stations. Analyzing the physical character is tic sand images of the devices might reveal patterns that appear strange or suspicious.

Differentiating Elements: Credit cards come equipped with tamper-evident features such as security labels and holograms. Graphics analysis can help determine whether these parts have been tampered with, adding an additional layer of safety. Visual Authentication : An increasing number of credit near issuers are looking at the usage of complex visuals and aspects for authentication and anti-fraud purposes. Verifying the authentic city of a card might beaded by looking at these visual elements.

Enhanced Customer Verification: Graphics analysis can be used in conjunction with other identifying methods, such as biometrics or Pins, to boost security and reduce the like LaHood of identity theft. Collaboration with Card Manufacturers: Credit card companies should work closely with card manufacturers to provide unique graphical aspects that will make it more difficult for fraudsters to create counterfeit cards.

V. Reducing the Risk of Lost or Stolen Credit Card Fraud: By examining the physical credit card and verifying its authenticity prior to being used for transactions, issuers can reduce the risk of lost or Stolen credit card fraud.

LITERATURE REVIEW

Analyze how graphical components—like holograms, logos,carddesigns,and other visual security measures—help detect credit card fraud. Investigate the techniques co artists employ to manipulate or fake these images.

Methods for Maintaining Confidentiality in Visual Analysis: Describe the privacy-preserving methods that graphics analysis uses to protect cardholder data and identify fraudulent behavior. Machine Learning and Visual Analysis: Analyze the ways in which credit card the fame be detected using visual analysis using machine learning approaches. Analyze studies that look into how effectively different machine learning systems identify fraudulent transactions using visual clues. Unbalanced Data Processing: To address the pervasive issue of class imbalance in fraud detection datasets, particularly with regard to credit card fraud detection, research should be done.

Investigate research on real-time transaction monitoring systems that employ visual analysis to spot possibly fraudulent transactions as they happen.

VI. GRAPHICSANALYSIS

The use of visual analysis in credit card fraud detection involves looking at the outward, palpable aspects of credit cards to identify any irregularities, discrepancies, or other signs of fraud or manipulation. This study greatly enhances the security of credit card transactions. The following are some essential components of visual analysis for identifying credit card fraud:

Finding Fake Cards: To assist identify fake credit cards, graphic analysis looks at visual elements such typefaces, holograms, logos, and card designs. Upon close examination, minute variations that are often seen in fake cards can be found.

Tamper Evident Features: Two types of tamper-evident features on credit cards are security labels and holograms. Figuring out whether the card has

undergone significant alteration or if these attributes have been changed.

Cloning Detection: By stealing the magnetic stripe information from authentic credit cards and maybe changing the card's appearance, thieves can replicate credit cards. Differences between the encoded data and the actual card's design can be found through graphic analysis.

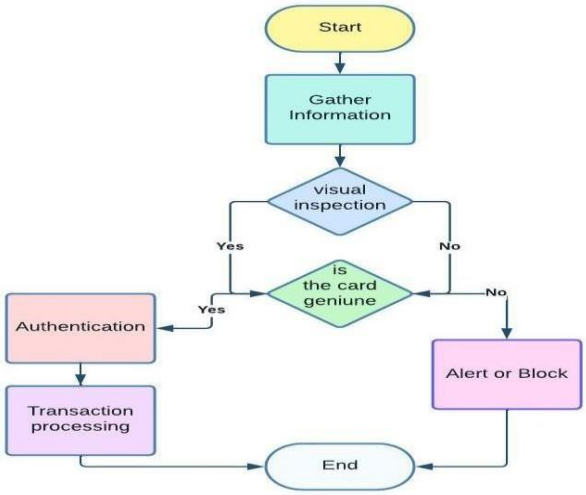
Fraud stars have the ability to manipulate point-of- sale (POS) terminals by changing their look, among other things. Modifications or discrepancies that can point to skimming efforts can be found with the use of graphic analysis.

Visual Authentication: For the aim of authentication and fraud prevention, several credit card issuers include sophisticated graphical elements. When processing transactions, graphic analysis plays a crucial role in confirming the legitimacy of these visual aspects.

Cloning Detection: Thieves can copy credit cards by replicating their magnetic stripe data and perhaps altering the card's design. Graphic analysis can identify discrepancies between the encoded data and the actual card design.

Aside from other things, fraudsters can alter the appearance of point-of-sale (POS) terminals. Graphic analysis can be used to identify changes or discrepancies that may indicate efforts at skimming.

tracking, and more to successfully identify fraud. When financial institutions and merchants extensively examine the visual elements of credit cards, they may identify potential fraud and take the appropriate measures to protect cardholders and halt illicit transactions.



VII. PRIVACY-PRESERVINGTECHNIQUE

Visual Authentication: A number of credit card issuers use complex graphical features in order to prevent fraud and verify identity. Graphic analysis is an essential component of transaction processing since it verifies the authenticity of these visual elements. Together, credit card companies and card makers may provide unique graphical features that are hard to replicate. Credit security may be enhanced by certain traits.

Enhancing Multi-Factor Authentication: Graphics analysis may be used in conjunction with other authentication methods, such as biometrics or PINs, to provide an additional layer of security and reduce the risk of identity theft.

Graphic analysis is typically used in concert with other techniques including machine learning algorithms, behavior analysis, transaction

Credit card fraud detection methods that respect privacy, including graphics analysis, can spot fraudulent behavior without jeopardizing the security of private cardholder information. Graphics analysis combined with the following privacy-preserving techniques can detect credit card fraud:

Symbolization: The process of replacing sensitive data, such as a credit card number, with randomly generated token is known as tokenization. The original card number can be hidden by graphics analysis applied to the tokenized data.

In addition to protecting cardholder data, this enables fraud detection by utilizing card design. SMP Stands for Secure Multi-Party Computation. With this method, group data analysis is made possible without disclosing the underlying data to out side parties. Credit card fraud may be detected

With the use of graphics analysis with out disclosing personal card information.

Calculations on encrypted data are made possible by the use of homomorphism encryption. Images of credit cards may be encrypted, and the encrypted In this approach, sensitive information is kept private.

Differential privacy: This technique adds additional noise to the data in order to protect personal information. It can safeguard privacy in graphics analysis by masking certain characteristics but leaving others visible so patterns can be found. Data does not require decryption in order to be analyzed.

VIII. PROPOSEDMETHOD

In this review work, we found that supervised learning is widely used by academics. SVM, KNN, and graphics analysis are frequently used. We also find that using a visual analysis works better than using only one algorithm or classifier. Numerous tests on the CCFD in the section above demonstrate the effectiveness of several machine learning models in this process; yet, the data's variability and imbalance persist. It's never easy to do CCFD, and models can never yield findings that are more accurate.

Because banks and other financial institutions have to comply with GDPR requirements, data heterogeneity and imbalance may be more of a problem when it comes to higher-risk privacy concerns. The recommended approach suggests protecting privacy while utilizing the datasets for effective ML model training.

IX. OPTIMIZATION

Before we can execute our formal model, we need to fix a distribution for transaction amounts. Using around 12 million transactions from online banking and 1.2 million from mobile banking, we used log normal distributions to estimate the distribution for both channels. It will be noted that, despite this option paying less attention to the distribution's tails, the optimal model still heavily emphasizes the identification of anomalies with large transaction amounts.

X. RESULTANDDISCUSSION

For the purpose of detecting credit card fraud, machine learning models and transaction data analysis are typically employed, with graphics analysis acting as a backup. Alert Triggered: A transaction begins with a credit card that appears genuine on the surface, but some visual elements, such as the hologram, have minute irregularities that are hard to notice with the unaided eye. Graphics Analysis: The system amines the given card design visually by using a database of legitimate credit card designs as a reference. It recognizes difference sin the placement of the logo, the hologram, or other visual security components. Transaction Data Analysis and Machine Learning: In addition, the system analyses transaction-related data simultaneously, including location, day of the week, transaction frequency, and cardholder behavior. The transaction is found to be inconsistent. alarm Generation: Based on the findings of the graphics analysis and the transaction data analysis, the system raises an alarm, marking the transaction as potentially fraudulent.

Review and Confirmation: A fraud analyst assesses the detected transaction and confirms the suspicion based on the results of visual inspection and transaction data analysis. Preventive Action: The fraudulent transaction is prevented from being allowed by stopping the transaction. The cardholder is promptly notified of the dubious behavior.

Conclusion

The different CCFD techniques that have been used are examined in this review research. The research shows that applying machine learning techniques to increase CCFD accuracy is a great idea. Inspire of this, large datasets are required for model training to avoid data imbalance. Using real- time data baseball lows us to access a greater variety of data, but privacy issues still need to be addressed.

Using the real-time datasets, we can train the model in a privacy-preserving manner thanks to our proposed method. An ANN used in a federated learning architecture can help the machine learning model detect fraudulent transactions more accurately. The proposed hybrid technique can

Successfully modify the way CCFD functions and provide new opportunities by utilizing real-world datasets. The suggested approach can guarantee that banks and financial institutions must collaborate.

to make effective use of the real-time datasets in order to help both sides in the creation of a successful CCFD system. The proposed method has limitations in terms of practical implementation, even if it successfully achieves CCFD while maintaining privacy by using the real-time datasets. All banks and other financial institutions have policies and procedures that they strictly adhere to.

Because banks and other financial organizations have their own limits and rely more on internal resources than on a centralized plan, it will be challenging to change the recommended method. Even a trained algorithm will ultimately detect patterns that hackers might be able to decode,even in the absence of central data exchange.Therefore, even with the limitations in place,effort still has to be done to convince banks and other financial institutions to use this technology.

REFERENCE

Lucas Y, Portiere P-E, Laborite L, et al. Multiple perspectives HMM-based feature engineering for credit card fraud detection.
In: ACM, 2019.

2. Duman E, Elikucuk I. Solving credit card fraud detection problem by the new metaheuristics migrating birds optimization.
Berlin:
Springer;2013.
3. BotcheyFE,QinZ,Hughes-LarteyK.Mobile money fraud pre-
diction—a cross-case analysis on the effciency of support vector
machines,gradient boosted decision trees,and Naïve Bayes
algo- rithms.
Information.
4. Rtayli N, Enneya N. selection features and support vector machine for credit card risk identifcation. Procedia Manuf.
5. Vynokurova O, Peleshko D, Bondarenko O, Ilyasov V, Serzhantov
V, Peleshko M. Hybrid machine learning system for solving fraud detection tasks. In: 2020 IEEE third international conference on data stream mining & processing (DSMP), IEEE; 2020.
6. Visacreditcardsincirculation2020|Statista.
7. SchetininV,JakaiteL,KrzanowskiW.Bayesian learning of models for estimating uncertainty in alert systems:
applicationtoair
8. traffic confict avoidance. Integr Comput Aided Eng.
2018;26:1–
9. https://doi.org/10.3233/ICA-180567.

10. Jakaite L, Schetinin V, Hladuvka J, Minaev S, Ambia A, Krzanowski W. Deep learning for early detection of pathological changes in X-ray bone microstructures: case of osteoarthritis. Sci Rep. 2021.
11. Supervise dandun supervised learning.In:2020 5th IEEE international conference on big data analytics (ICBDA).
IEEE; 2020.
12. . Li W, Lin S, Qian X, et al. An evidence theory-based validation method for models with multi variate outputs and uncertainty.
13. ZiębaM,TomczakSK,TomczakJM.Ensemb le boosted trees with synthetic features generation in application to bankrupt cyprediction. Expert Syst Appl.
14. VynokurovaO,PeleshkoD,Bondarenko O, et al. (2020) Hybrid Machine Learning System for Solving Fraud Detection Tasks.