EasyChair Preprint

№ 4664

Fraudulent Activity Detection System in Banking Sector

Tilesh Deshmukh, Sayali Chaudhari, Damini Marathe,
Shweta Pawar and Mayuri Kulkarni

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

November 27, 2020

Fraudulent Activity Detection System in Banking Sector

Tilesh Deshmukh[1], Sayali Chaudhari[2], Damini Marathe [3] Shweta Pawar [4], Mayuri Kulkarni[5]
[1]*Department of Computer Engineering, SVKM's Institute of Technology*
Dhule, India

[1]dtilesh@gmail.com;[2] sayalichaudhari158@gmail.com;
[3] daminimarathe1999@gmail.com; [4]shwetapawar75565@gmail.com; [5] mayuridkulkarni@gmail.com

Abstract - ***Online transaction is becoming a major payment method in many countries. However, the rate of payment fraud with call is higher than with credit card. One potential reason is that call detail is easier to be modified than credit card data by fraudsters, which degrades our data-driven fraud detection system. Supervised learning methods are pervading used in fraud detection. However, these supervised learning methods used in fraud detection have traditionally been developed following the assumption that the environment is benign; there are no adversaries trying to evade fraud detection system. In this paper, we took potential reactions of fraudsters into consideration to build a robust fake call detection system using adversarial examples. Experimental results showed that the presentation of our proposed method was improved in both benign and antipathetic environments.***

Keywords — Phishing frauds, Fake call frauds, fraud transaction detection system, Block chain method, confidential disclosure agreement, Location, real-time Fake call fraud detection

I. INTRODUCTION

The online transactions have been increased significantly in recent years, unfortunately so has fraud, which fraud is billion-dollar business and it has increased for several years. Credit or debit card fraud is the most popular items for thieves among many frauds because many customers personal message is suffered from leakage. It is accessible for hackers (unauthorized) to give the information about the password or security number from consumers (bank authorized user) and transfer money to their accounts. Fraud detection plays an important role in minimizing these losses.

Nevertheless, fraudsters continue their invasion by defeating all the existing and newly developed anti-fraudulent techniques with their clever dodging. In this study we focus on real-time fraud detection of digital Banking transactions (called phishing fraud) (e.g., logins, payments, view statements).

Phishing is a type of communal engineering attack often used to appropriate user data, including login credentials and credit card numbers. It occurs when an attacker, simulate as a believe in any entity, duplicate a victim into opening an email, instant message, or text message.

The purpose of a fraud detection solution in this setting is to assess in real-time the risk of each individual transaction in the form of a fraud probability. Then the bank may choose to allow the transaction, deny the transaction or impose some form of authentication on the user upon successful completion the transaction will be allowed.

Security is one of the major concerns of e-banking transaction people using e-banking are worrying that intruders will get into their account and spend their money.

China's e-banking fraud case has entered a period of fast growth and the risk of e-banking transaction is rapidly improving according to the report 29.17% of phone fraud happened.

II. LITERATURE SURVEY

Fraud act as the wrongful or criminal deception intended to result in financial or personal benefit. It is a deliberate act that is against the law, rule or policy with a aim to attain unauthorized financial benefit. Lokesh Sharma ans Raghavendra Patidar works on emerging technology Neural Network that can be used in banking or financial areas to detect fraud. They have been successfully applied to detect legitimate or fraudulent transactions. Association Rules can be applied to detect fraud this proposed Methodology has been applied on data about credit card fraud of the most important retail companies in Chile. In the area of fraud detection, neural network like feed forward neural network with back propagation have found immense application. Usually such applications need to know previous data and on the behalf of this previous data they detect the fraud.

They focused on a solution to minimize the wrongly classified transactions. They merge the Meta heuristic approaches scatter search and genetic algorithm. Peer group analysis made by David Weston and Whit row is a best resolution is regard to credit card fraud detection.

Ekrem et.al combined the genetic algorithm and Scatter search approach that is such a helpful to find abnormal transactions. David Weston gives a good resolution to detecting credit card fraud detection using generation analysis method. So, the main motive of our paper is to represent all important technologies that can detect the fraud as soon as possible and to ignore the loss as much as possible [1].

The fraud detection is a critical task and there is no system that correctly predicts any transaction as fraudulent. The properties for an ethical fraud detection system are:

1. Should identify the frauds accurately.
2. Should detect the frauds quickly.
3. Should not classify a authentic transaction as fraud.

Outlier detection is a critical task as outliers indicate unusual running situations from which significant performance degradation may happen. Techniques used in fraud detection can be classified into two:

1) Supervised techniques where past known legal/fraud cases are used to build a model which will produce a intuition score for the new transactions.

2) Unsupervised are those where there are no prior sets in which the state of the transactions are known to be fraud or legitimate [2].

In "Credit Card Fraud Detection Using Hidden Markov Model" paper, they have suggest an application of HMM in credit card fraud detection. The different steps in credit card transaction processing are act as the fundamental debatable process of an HMM.

They have used the ranges of deal amount as the examination symbols, whereas the types of item have been considered to be states of the Hidden Markov Model. They have suggested a method for finding ZA the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been describe how the HMM can expose whether an incoming transaction is fraudulent or not. Exploratory results show the performance and efficacy of our system and illustrate the functionality of learning the spending profile of the cardholders. Comparative studies disclose that the Accuracy of the system is close to 80 percent over a broad variation in the input data. The system is also extensible for handling large volumes of transactions [3].

In "credit card fraud detection with a neural network" paper, using data from a credit card issuer, a neural network based fraud detection system was instruct on a large sample of labelled credit card account transactions and tested on a arbitrator data set that consisted of all account activity over a ensuing two-month period of time. The neural network was trained on examples of fraud due to lost cards, thieve cards, appeal fraud, copied fraud, mail-order fraud and NRI (non-received issue) fraud. The network detected remarkably more fraud accounts (an order of magnitude more) with notably hardly any false positives (reduced by a factor of 20) over rule based fraud detection plan of action. The system has been installed on an IBM 3090 at Mellon Bank and is presently in use for fraud detection on that bank's card folder [4].

In "Offline Internet Banking Fraud Detection" paper. Motive of this paper is to illustrate one successful fraud detection model which is accepted in Greece.

Aside from the offline internet banking fraud detection system itself, which is concise, there scope is to present its contribution in quick and good detection of any "unusual" transaction including fraudulent ones [5].

In "Security Analysis for Internet Banking Models" paper they express that Internet banking fraud can be performed internally by authentic staff or externally by customers or suppliers. This paper presents a secure analysis of the proposed Internet banking model compared with that of the contemporary existing models used in fraudulent Internet payments detection and avoidance. However, they have no effective detection mechanism to identify legal users and trace their illegal activities. The present model facilitates Internet banking Fraud Detection and avoidance (FDP) by applying two new secure tool, Dynamic Key Generation (DKG) and Group Key (GK) [6].

In "Study on Fraud Risk Prevention of digital banking sector" paper .The main motive of this paper, in the first hand, at argument on the fraud risks of online banking, introducing the ongoing application situation of information sharing mechanism in respect of internet fraud outside China as well as the development of such idea in China.

Then, a system is map-out for sharing online fraud information. The paper family proposing that all the online banks should put more joint efforts in perfecting this mechanism for sake of international co-operation [7].

In "Fraudulent Internet Banking Payments avoidance using Dynamic Key" In this paper, they have present a well-organized new scheme which can avoid fraud by applying different safety algorithms, creating and modernize limited-use secret keys.

It uses up-to-date testimonial technologies and is well modified to any possible future technology. Moreover, it does not depend on fixed values where hacking one secret will not understanding the whole system's security. The peer group of each set of keys is based on dynamically generated liking keys.

For future work, we aim to analyse the security of the system that applies the proposed technique. Moreover, we aim to apply the present technique to other kinds of internet applications, especially mobile commerce [8].

A parallel granular neural network (GNN) is expand to speed up data mining and knowledge discovery procedure for credit card fraud detection.

The data are classed into three categories: first for training, second for forecast, and third for fraud detection. After learning from drilling data, the GNN is used to forecast on second set of data and later the third set of data is concern for fraud detection. Around eight scenarios are employed for detecting our motive.

GNN gives fewer average training bugs with larger amount of previous training data. We also found that the number of training bugs is inversely proportional to the number of training cycles. The elevated fraud detection error is, the greater possibility of that transaction being actually fraudulent [9].

III. PROPOSED METHODOLOGY

Fraud transactions have become a widen problem in the online banking domain. As technology progression, fraud peoples also change their methods of executing frauds. There are also emerging technologies that allow fraudsters to mimic the transaction behaviour of genuine customers and they also keep changing their methods so that it is difficult to detect fraud. Sometime happens the fraud like fake calls and getting information like credit card details or banking details. And to detect that problem we design this system. So we design this advanced system to detect that fraud by tracking their location.

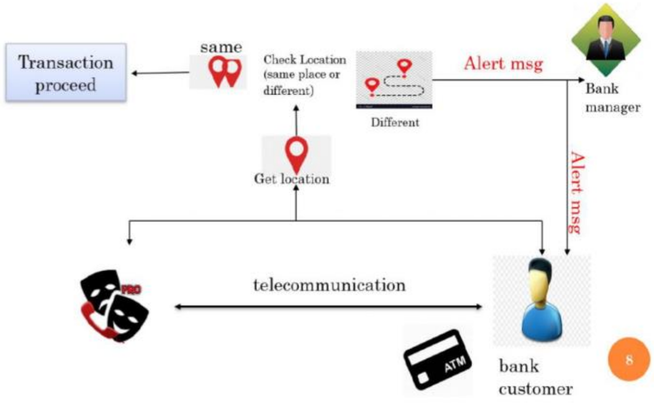

Fig 1: Graphical Working Diagram

IV. FLOWCHART

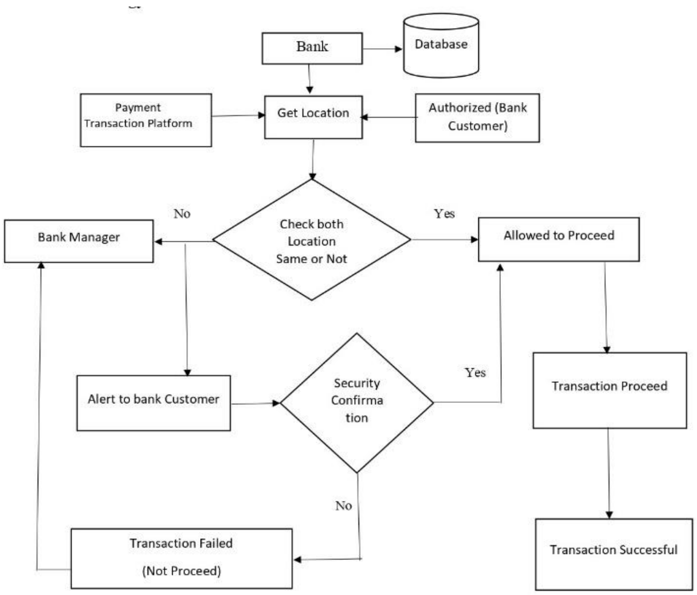

Fig 2: Propose System Pictorial Flowchart

Represents a sample scenario of transaction process. In these all the information of authorized user is store in the bank section eg. (Name, Address, Card number, Credit card information) After that it goes to get location section and checks the location of authorized user who enters the all information of credit card. And payment transaction platform means where the payment will be withdrawal or deposits from account it is online either offline then next it checks both locations are same or not. If both locations are same then transaction will be proceeding. If both locations are not found same then alert message will send to bank customer as well as bank manager. If bank customer sends the positive reply to the alerting message then security confirm that transaction are allowed to proceeding when transaction proceed in these particular section verify this transaction and ask to authorized user to proceed or not. When transaction proceed in these particular section. Methodology in block chain is used for hiding actual data so fraudster's can't stole the data easily for hiding data in block chain we use hash function. Hash function converts a zip letters and numbers into an encrypted output. So it is very useful.

Then, bank customer neglects to proceed for the transaction using the alert message. For transaction we need then OTP (One Time Password)not sends to bank customer and transaction will be denied stores the alert message to bank manager side because of in future we need the bank customers account information in case any problem occurs.

V. EXPECTED OUTCOMES

We bring together different strategies to predict and detect online banking fraud. In this we can easily detect fraud by tracking their geo-location. The proposed method allows transparency to its decision by extracting and comparing geo-location of the device. If there is any ambiguity in terms of both the location of user as well as the person performing transaction, user is alerted with message and the transaction is denied**.** So in this way we can stop the big loss.

VI. CONCLUSION

Online banking activities are constantly increasing and are likely to become even more common as online banking platforms develop. One side effect of this drift is the rise in attempted fraud. We propose a consciousness based architecture for classifying digital banking transactions as either fraudulent or genuine. The proposed method allows transparency to its decision by extracting and comparing geo-location of the device. If there is any ambiguity in terms of both the location of user as well as the person performing transaction, user is alerted with message and the transaction is denied.

REFERENCES

[1] Dingling Ge,Shunyu Chang,Jianyang Gu,JingHui Cai, "Credit Card Fraud Detection Using Lightgbm Model", International Conference on E-Commerce and Internet Technology,2020.

[2] Dhiman Sarma,Wahidul Alam,Ishita Saha,Mohammad Nazmul Alam,Mohammad Jahangir Alam,Sohrab Hossain, "Bank Fraud Detection using Community Detection Algorithm", Proceedings of the Second International Conference on Inventive Research in Computing Applications ,2020.

[3] Simon Delecourt,Li Guo,"Building a robust mobile payment fraud detection system with adversarial examples",IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering,2019.

[4] Idan Archituve, Sarit Kraus, Jacob Goldberger,"Interpretable Online Banking Fraud Detection Based On Hierarchical Attention Mechanism", 2019.

[5] Mr.Sunil S Mhamane, Mr.L.M.R.J Lobo,"Ineternet Banking Fraud Detection Using HMM", IEEE,2018.

[6] Chaonion Guo,Hao wang,Hong-Ning Dai,Shuhan Cheng,Tongsen Wang,"Fraud Risk Monitoring System for E-Banking Transactions", IEEE 16th Int. Conf. on dependable, ascetic & Secure Comp., 16th Int. Conf. on extensive Intelligence & Comp., 4th International Conf. on Big Data Intelligence & Comp., and 3rd high-tech Sci. & Tech. Cong,2018.

[7]Samuel Ndueso John,Kennedy Okokpuje,Funminiyi Olajide,"Fraud Detection in Banking Sector Using Data Mining Techniques/Algorithm",International Conference on Computational Science and Computational Intelligence, 2016.

[8] P.Jayant,Vaishali,D.Sharma,"Survey on Credit Card Fraud Detection Techniques",International Journal of Engineering Research & Technology,2014.

[9] L. Fang, M. CAI, H. Fu, and J. Dong, "Existential-Based Fraud Detection," in Computational Science – ICCS 3112, pp.1048-1055, 2013.