IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, June 2022

Critical Analysis of Online Transaction Frauds

Nimisha Vikram Gaikwad[1] and Prof. Divakar Jha[2]
Student, Department of MCA[1]
Guide, Department of MCA[2]
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Nowadays, bank transactions are carried out on a large scale which is very complex and time-consuming. It is not possible for banks to perform those transactions manually like in ancient day's banks. Thus, there arises the need for IT to handle lengthy and complicated transactions in the banks. IT has made banking procedures easy, convenient, quick, and professional, which is one of the greatest landmarks in banking history. Internet banking is now becoming the most commonly used form of banking transaction. With the rise in online transactions, we tend to conjointly observe a significant increase in the number of fraud cases, leading to billions of dollars in losses each year worldwide. The issue of transaction fraud could be a major source of concern. Therefore, it is vital and necessary to develop and apply techniques that can assist in fraud detection and prevention.*

Keywords: Fraud, Online Transaction, Security, Prevention, Detection

I. INTRODUCTION

Information technology plays a significant role in the banking sector. Day by day increasing modifications in the technology world led to improve e-banking services of assorted banks. The ancient branch model of banks is currently turning into a new kind of e-banking service. It provides varied benefits to customers of various banks. Nowadays individuals are educated more than in older days. Today human lives become machine oriented and they don't have enough time to visit bank branches than ever before. E-Banking means providing banking merchandise and services through electronic delivery channels like ATM, Internet banking, telephone banking, and other electronic delivery channels. Automated Teller Machine-ATM is an electronic computerized telecommunication device that permits a client to directly use a secured technique of communication to access their bank accounts or make cash withdrawals and other services. Internet banking is extremely helpful to customer who has a computer with an internet connection, they don't have to visit a bank branch for their business transactions. Simply they can transact anywhere, anytime if they have an internet connection. Internet banking enables one to shop for and sell without physical cash, make deposits, transfer, pay bills, etc. with ease.

Recently we have observed a significant increase in the volume of electronic transactions, mainly due to the popularization of the World Wide Web and electronic commerce, like online retailers (e.g., www.ebay.com, www.walmart.com, www.amazon.com).

The rapid development witnessed in global information infrastructure over the past few decades, particularly within the areas of computer and information technology (telecommunications systems and the Internet) has brought electronic commerce development to a global stage. These developments have facilitated the effective interaction between business individuals and their customers, and with other corporations within and outside their industries

Electronic banking is driving the globe toward cashless banking. Though electronic banking is beneficial to the banking industry, it has also introduced great security threats to banks and their customers. There is a significant increase in the number of fraud cases, leading to billions of dollars losses annually worldwide. Fraud is illegal action performed for a particular motive like to gain money, goods, services, and sometimes fame, etc. Fraud exists in our society since ancient times. However, the ways of doing fraud are also enhanced with time. Frauds are acutely increasing with the progress in technology and worldwide communication. Transaction frauds are taking place more often than ever before, particularly in today's Internet era, and it causes huge financial losses.

Electronic banking makes use of access codes, which is in the form of Personal Identification Number (PIN) before access is granted to the user of the bank services. This has not invariably saved the banks from the antics of fraudsters, fraudsters use varied avenues to divulge or steal customer's secret access codes which they personalize, and use the

DOI: 10.48175/568

opportunity to impersonate and rob their victims of their valuables from the bank. Some robbers confiscate ATM cards from owners with their PINs, seize tokens and other electronic banking applications access codes; which they use in defrauding their victims. Many banking customers resist electronic banking for fear of being defrauded. Some internet thieves use phishing and spooling to bait their victims. Bank customers who do not seek verification from their banks easily fall prey.

II. LITERATURE SURVEY

[1] in this paper author Mostafa et. Al reviews all methodologies of previous research work but there is no current single method that will be efficient in the detection and prevention of all kinds.[2] The author proposes a novel credit-card fraud detection system by detecting four different patterns of fraudulent transactions using best suiting algorithms and by addressing the related problems identified by past researchers in credit card fraud detection. By addressing real-time credit-card fraud detection by using predictive analytics and an API module the end user is notified over the GUI the second a fraudulent transaction is taken place. Therefore, we can conclude that there is a major impact of using resampling techniques for obtaining a comparatively higher performance from the classifier. The machine learning models that captured the four fraud patterns (Risky MCC, Unknown web address, ISO Response Code, Transaction above 100$) with the highest accuracy rates are LR, NB, LR, and SVM. [3] Authors have applied and evaluated four different computation intelligence techniques, after choosing them from an initial set of evaluated experiments that adopt several distinct techniques. In order to evaluate the techniques, we apply them in an actual dataset, containing thousands of transactions per day, from the most popular Brazilian electronic payment service, called PagSeguro. Confidentiality can be compromised in the process of electronic purchases [4] in this paper author has introduced a new approach to prevent threats during online transactions in order to protect information through a two-step mechanism of authentication. The primary step of authentication is OTP verification. If the OTP has been checked, the face should be recognized. [5] This paper discusses various strategies for detecting fraud in online transactions. It provides an overview of many research papers in the subject of online transaction fraud detection that may be used to successfully address challenges that arise in the detection and prevention of fraud. In future research, machine learning algorithms will be utilized in conjunction with various input and output variables to detect fraud in online transactions.[6] The behavior-based classification method using SVM is used in this project. The suggested approach offers greater identification precision and is also scalable for managing large quantities of transactions. [7] In this report, for online transaction fraud detection, deep Representation of Learning Model is proposed, which has the benefit of achieving strong and stable results.[8] In this paper proposal of smart software which can track suspicious textual messages and audio conversations along with detection of malafide software agents, one proposal of development of intelligent software agent is also very important which may be self-evolvable and can track source of fraudulent and nullify the effects of these and it may be helpful to nab fraudsters too.

III. TYPES OF ONLINE TRANSACTION FRAUDS

Scammers have become skilled in illegally collecting data online. Hackers often pretend as legitimate people and contact card owners asking for sensitive details and information. They then use several ways, as mentioned below, to interact and steal crucial data.

- Email
- Messages
- Illegal websites
- Phone calls
- Sending malicious software to smartphones

Cybercriminals often operate in teams to breach data security systems. They check for bugs or fixes that have not been updated in quite some time. Such loopholes make it easy for hackers to gain access around the firewall and acquire confidential information.

Some of the common types of attacks include

- **Phishing:** This occurs when an attacker impersonates a server on a website by setting up a fake version of the targeted website; this website version can contain all the code of the original website. Then, the attacker uses the fake website to send messages to several email accounts to trick the message recipient into visiting the

DOI: 10.48175/568

spoofed website and reveal their login details.

- **Cloned voice-banking systems:** This is a situation where an attacker clones the voice-banking systems to make them sound like the official systems. This form of attack uses fake e-mails to solicit customer calls to a fake phone number.

Triangulation fraud requires three different types of actors: the person doing the fraud, a shopper, and an eCommerce store. The fraudster sets up a storefront (on Amazon, Shopify, or another platform) that sells high-demand goods at competitive prices.

Setting up this storefront brings in a number of legitimate customers who are looking to take advantage of an incredible bargain. Once these customers place orders on the fraudster's website, the fraudster uses stolen credit card numbers to purchase legitimate goods from your eCommerce website, and then send those goods to their customers.

While the customers of the fraudster's store may be receiving real goods for an unbelievable price, the victims are (1) those whose credit cards have been stolen and (2) your eCommerce website. Your eCommerce store ships real items to the fraudster after they use stolen credit card information to place these orders.

Interception fraud is when fraudsters place orders on your eCommerce website where the billing address and shipping address match the information linked to a stolen credit card. Once the order is placed, their goal is to intercept the package and take the goods for themselves.

This can be done in several ways. First, they may ask a customer service representative at your company to change the address on the order before it is shipped. By doing this, they aim to receive the goods while the actual payment is made by the victim. They may also contact the shipper (whether it is FedEx, UPS, or another courier) to reroute the package to an address of their choosing. If they live close to the victim, they may even wait for the physical delivery of the package, sign for the package, and take it for themselves.

- Stolen or lost credit/debit card and its abuse by fraudsters.
- Cloning of debit/credit cards.
- Stolen PIN numbers and banking passwords
- Hacked accounts and mobile apps
- Stolen CVV and OTP number.
- Online shopping frauds. In such cases, fraudsters set up fake online shopping platforms.
- Luring people to share their confidential information like AADHAR details, ATM PIN, an account password, etc. in the name of some attractive gifts or lottery and duping money thereafter

IV. CONTROLLING E-BANKING FRAUD

Electronic fraud is committed using communication platforms and can be controlled using the same medium. Information technology utilizes full computer technology, which is the brainchild of communication. Computer security which is concerned with the protection of computer resources and infrastructure from misuse, theft, corruption, and natural disaster to make them remain accessible and functional to the user, is one of the media through which electronic banking fraud can be controlled.

Following ways can be measures to prevent fraudulent and sharp practices in the net

- **Encryption:** Encryption is used in data communication to convert data on transit or stored to an indecipherable form such that, the data will be meaningless to fraudsters in the cause of interception. The policy here is that it is only the owner of the message that can decrypt the data and make it meaningful. Microsoft and Netscape email programs have synCrypt and SIMIME encrypting programs used in their data communication.
- **Firewalls:** Firewalls is used in computer to block suspicious programs from running on the system, thereby, denying the suspicious programs control or access to the system.
- **Access point cloaking:** this has to do with the configuration of access points, such that, request to connect from unknown sources are not responded to.
- **Access authorization:** Access authorization is a program that masquerades the access point requesting authority, or permission to access an application or the net.

The user will be expected to enter the necessary requirements in the form of PIN (Personal Identity Number), user name, password, or biometrics as the case may be before access is granted.

Use of anti-virus software to debug viruses and malware

Use of cryptography to transform data or information before transmitting, so that an unauthorized person who intercepts it cannot decipher it. Only the sender and the authorized recipient can decipher the message.

- **Use of Biometric authentication:** Biometric is the measure of physical features or behavioural patterns of individuals. The physiological features scan is analysed using a mathematical algorithm. The analysed physiological feature is stored in the database in the form of data (minutiae), which is used to verify and authenticate the person in a subsequent transaction,
- **Legislations and policies:** The promulgation and implementation of legislations, and policies prohibiting electronic fraud with stipulated punishment for culprits, is a very important control measure for electronic fraud. Humans are complex and trivial in behaviour. When given the opportunity to control themselves, they find it difficult to do the right. As such needs documented control measures that control their behaviours against excesses. Such a document should clearly specify the punishment meted for any misconduct. As a matter of necessity and precedence, offenders should be made to face the consequences of their misconduct as stated in the Constitution. If this is enforced, humans are expected to shape their behaviour to suit well in such a society, if this is equally implemented in electronic fraud, it should be a good control measure then.

Cyberthieves also work in teams to penetrate network security systems by looking for glitches or patches that haven't been updated in a while. These gaps give hackers access around a firewall and make it easy to illegally obtain sensitive information.

V. CONCLUSION

Electronic banking has helped greatly in providing banking services with ease and efficiency globally. It has reduced time waste and high charges associated with the traditional banking system. It has led to banking-as-you-go, and encourages cashless banking. Fraudsters have as well taken advantage of the platform to perpetrate serious crimes that affect both the bank as an institution, and the bank customers. This paper provides an overview of many research papers in the subject of online transaction fraud detection that may be used to successfully address challenges that arise in the detection and prevention of fraud. This paper provides an overview of many research papers in the subject of online transaction fraud, that may be used to successfully address challenges that arise in the detection and prevention of fraud. In this report on online fraud detection, integration of biometrics in electronic banking, creation of smart software which can detect suspicious textual messages and audio conversations along with detection of malafide software agents, and development of intelligent software agent which may be self-evolvable and can track the source of the fraudulent are proposed.

REFERENCES

[1] Mostafa A. Alia, Nazimah Hussinb, Ibtihal A. “E-banking fraud detection- a short review”

[2] Anuruddha Thennakoon1, Chee Bhagyani2 , Sasitha Premadasa3, Shalitha Mihiranga4, Nuwan Kuruwitaarachchi5 “Real time fraud detection using machine learning”.

[3] Evandro Caldeira, Gabriel Brandao, Adriano C. M. Pereira “Fraud Analysis and Prevention in e-Commerce Transactions”.

[4] Ashwini.M. Zinjurde, Vilas.B.Kamble “Credit Card Fraud Detection and Prevention By Face Recognition”

[5] Virjanand, Rajkishan Bharti, Shubham Chauhan, Suraj Pratap Singh ” A Comparative Study on Online Transaction Fraud Detection by using Machine Learning and Python”

[6] I.Mettildha Mary, M.Priyadharsini, Dr. Karuppasamy.K, Ms.Margret Sharmila.F “Online Transaction Fraud Detection System”

[7] J Fenila Naomi, Roshan Jeniel R, Sakthi Eswaran K, Sanjeev Kumaar N M “Intelligent Transaction System for Fraud Detection using Deep Learning Networks”

[8] Surbhi, Dr. Sanjeev Kumar “Fraud Detection During Money Transaction and Prevention”

[9] Dr. Eneji, Samuel Eneeji; Angib, Maurice Udie; Ibe, Walter Eyong; Ekwegh, Kelechukwu Chimdike “A Study of Electronic Banking Fraud, Fraud Detection and Control” (2019)