RESEARCH ARTICLE

ADHYAYAN Volume 12, Issue 1, 2022 Print ISSN: 2249-1066 Online ISSN: 2455-8656

A Review of Literature Based Online Fraud in India

Smita Tripathi*, Narendra Sharma

Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Pachama, Madhya Pradesh, India

Abstract

The purpose of the study is how the different researcher fraud can be predicted in the online transaction of data. Data analysis is an important part of fraud detection because data transformation into valuable information can result in competitive business advantages. The implementation of fraud prediction in any type of transaction on big data is one of the most important approaches applied by banks to using this approach, they shield their transaction, which is the Flow in the network. Fraud is an elementary problem with every financial institution in the word. Fraud has been a million-dollar business that is fastly growing at the international level.

Keywords: Big data, Financial institution, Fraud detection, Fraud prediction.

Adhyayan: A Journal of Management Sciences (2022); DOI: 10.21567/adhyayan.v12i1.9

Introduction

Online Fraud or Crime is not the newest dispute, but because of the Increasing of technology or the advent of e-commerce in 1995, online fraud increases with each passing year. It is mainly affected in the banking sector, Social media sites, online gifts, Internet ticketing, Purchase fraud, etc. Digitization is the main reason behind an increase in online fraud. This paper talks about different types of online fraud in India that are increasing and the causes behind any online fraud or Internet Fraud. This paper also explains the tools and techniques used by fraudsters. This paper also gives details concerning how online fraud is becoming an increasing threat for online retailers, customers, and businesses, dealing with online fraud, and avoiding the misuse of social networking sites or the Internet. This paper also provides the facts on the present status of online or cyber fraud, internet threats, and fraud and talks about the disputes that India needs to face to strike the internet risk.

Digital fraud has increased recently because of so many reasons involved, like the global COVID-19 crisis at that time, and everyone depended totally on digital media. At that time, retail purchases shifting online, the start of a new marketplace platform, payment was shifted to online mode, gradually increased digital banking services, more complicated fraud strategy, and scientific changes in technology.

Corresponding Author: Smita Tripathi, Department of Computer Application, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Pachama, Madhya Pradesh, India, e-mail: smita_mca2004@rediffmail.com

How to cite this article: Tripathi, S., Sharma, N. (2022). A Review of Literature Based Online Fraud in India. Adhyayan: A Journal of Management Sciences, 12(1):71-75.

Source of support: Nil

Conflict of interest: None

Purpose of Work

The purpose of this work is this concept provides a fraud management solution to avoid risk brought by unplanned circumstances. Fraud is one of the important hazards faced by business, banking, and financial sectors due to the nature of the operation.

Financial management solutions provide maximum security in the company's activities. Ensure that the companies use fluent and secure internal communication protocol to create a safe channel for detection and reporting.

Literature Review

Previous related work was done in the direction of fraud exposure.

(Singh, 2013) Fraud exposure is identifying fraud as soon as possible after it has occurred. Once fraud prevention has failed, fraud detection becomes

necessary. Fraud detection must be used continuously since one may not be aware that fraud prevention has failed. Whenever criminal discover a detection method has been implemented, they will change their approaches and try another. Day by day, new criminals are entering the field .many of them are not aware of the fraud detection method that has been very effective in the past and will try an alternative technique. This means that with the latest development, earlier detection techniques and tools are also required to be useful. This is not easy to develop new fraud prevention methods because exchanging thoughts or ideas in fraud detection is very narrow. It may be dangerous to express fraud prevention methods in detail in the public domain, as the criminal can take help from it.

(Murugan, 2012) Fraud is all about identifying and understanding the current situation and selecting prevention strategies based on cracking experience. Back in 2003, we nabbed an international criminal wanted by various Law Enforcement Agencies, including the FBI, and realized the scope of the plastic money fraud and the need for domestic measures. This method describes the nature of a situation at the time of the study and explores the causes and methods of frauds in plastic money to arrive at solutions. They utilize both primary and secondary data.

Data from the primary research was obtained through this new study. Using a questionnaire, we were able to collect data to study the behavior of card users. Researchers also avoided disclosing the participants' names or personal information in this research. A questionnaire was given to gather data to study the card user population and their behavior. The confidentiality of the participants was also assured by not telling their names or subjective information in the exploration. Research questions were answered only by relevant details. We have considered several different perspectives gathered from secondary data sources in developing the recommendations. Selections of cases were also dealt with in the secondary data during the research conducted in the city. The evolution of money from traditional to plastic has also seen the evolution of fraud from terrestrial to cyber, to be more specific, from robbery/theft to plastic money fraud. Conventional frauds are distinguished from this type by their ease of learning, low resources and lack of physical presence, and often ambiguous legality. Therefore, plastic money frauds pose new challenges for lawmakers, law enforcement agencies, and national and international institutions

(Thresiamma K. George, 2017) The monitoring, analyzing, detecting the vulnerabilities and preventing the attacks should be a continuous process so that the severity of the compromises or attempts on attacks can be mitigated. The security team and the system architects must also provide the best possible protection strategy. In the current scenario, most companies have the necessary protection device regarding firewalls and intrusion detection systems as part of their security infrastructure. However, many organizations do not have complete tools and practices to secure their applications.

Hence the hackers continue to attack the monitoring, analyzing, detecting the vulnerabilities, and preventing the attacks should be a continuous process so that the severity of the compromises or attempts on attacks can be mitigated. The security team and the system architects must also provide the best possible protection strategy. Hence the hackers continue to attack the application layer, and the application developers are focusing on the sophisticated features rather than removing vulnerabilities. Proactive and consistent risk management architecture can efficiently prevent, detect and remediate vulnerabilities in the application layer. As per the security report, it is not an ideal situation to keep track of thousands of known vulnerabilities by a single tool or a human developer. The best coding practices can be another solution to reduce vulnerabilities in the early stage. As per the detailed report by various security organizations, the Static Application Security Testing (SAST) tools can be an ideal choice to identify vulnerabilities in early-stage development by efficiently determining the vulnerabilities in each line of code. But it has an inherently higher false-positive rate than the Dynamic Application Security Testing tools (DAST). Most developers prefer to compile their code and dynamically test it in a run-time environment iteratively because some of the vulnerabilities will appear only in a run-time environment. In this situation, the DAST tools seem to be much more accurate (Akrout and Nicomette, 2014). Appropriate Server Configuration and necessary patches are important strategies for the prevention, detection, and remediation of vulnerabilities

(Richhariya, 2016) Adapting to the advancement of technology, the entire business sector has shifted to online services delivering e-commerce, information, and communication services to allow their customers better proficiency and convenience, thus increasing the number of online users exponentially. Modern

technology has simplified our day-to-day activities in several essential service sectors such as online shopping, electricity bill payments, mobile recharging, and other essential services. However, it has also made our lives more vulnerable to fraud attacks such as identity theft online, fraud on banks and credit cards, insurance frauds, and money laundering. The prevalence of fraud changes with the progression of social, financial, and technological developments and thus, takes on different forms and intensities based on the era. The development of current technology, global communications facilities, and the fraudsters' expertise has paved the way for a drastic increase in fraud occurrences and fraud losses. New fraud forms are appearing on the scene due to the attempt to find financial crime as part of a planned crime.

(Mudasir Ahmad Wani, 2019) Online Social Networks (OSNs) are an excellent platform to interact, collaborate and share content. OSNs have changed the way people think, express, and socialize with the outside world. Nowadays, there are a number of social networking sites like Facebook, Twitter, Flicker, LinkedIn, Research gate, etc., which are used by public to take out their social and professional activities. These OSNs can be classified into different categories based on the context of the functionalities they provide to the members, such as applications designed to build and maintain social connections, applications that focus on facilitating the sharing of media, or the application forums that allow people to share knowledge, news, and ideas. Nowadays, these networking websites are immensely utilized by users for sharing personal, professional, and political views, and therefore, these sites hold a massive content of one's life. Even though these sites have made people's social life better, there are several issues with using them, and the proliferation of fake accounts is one of them. These OSNs are appeared to be an attractive target of cybercriminals who create fake accounts to spread spam, defame, bully or troll a person, manipulate online voting or exploit the information crawled from their networks.

Researchers have proposed and implemented several techniques for designing a fake profile detection model, but these systems do not yield satisfactory results because of the inability to capture the varied behavior of different fake profiles. Hence, an efficient fake profile detection system is needed to combat and mitigate these fake profiles from OSNs. While working towards building a robust fake profile detection system, we encountered a number of challenges as discussed in this thesis. The Key contributions of this thesis are summarized in the following sections.

According to Booklet of Beware on the topic "Raju and forty thieves" produced by the Reserve bank of India in July 2021, it is based on financial fraduants. This booklet is an easily understandable pictorial description of incident happening around us. That helps us to learn how to keep hand-earned money and us safe from fraudsters. This booklet is a manifestation of our effort. The author provides us some tips about Do's and Don'ts in this booklet. They also explain how many online frauds are faced us by our daily life and also their precaution methods

The Figures 1 to 5 show some online fraud and scams, which we face in our daily lives. These figures show the different types of fraud differently.

Measures to Stay Safe Online Fraud

- Never make payments or share secure credentials for e-mails/lottery calls. Always doubt when you come across such unbelievable lottery or offers
- No need to enter your PIN/password anywhere to receive money
- Be careful while scanning any QR codes using payment apps. QR codes have embedded account

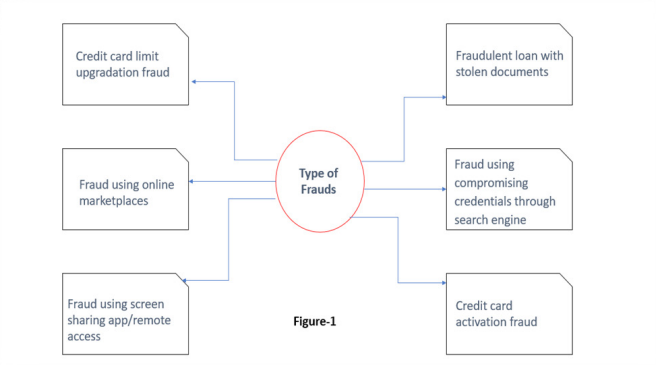

Figure 1: Types of fraud 1

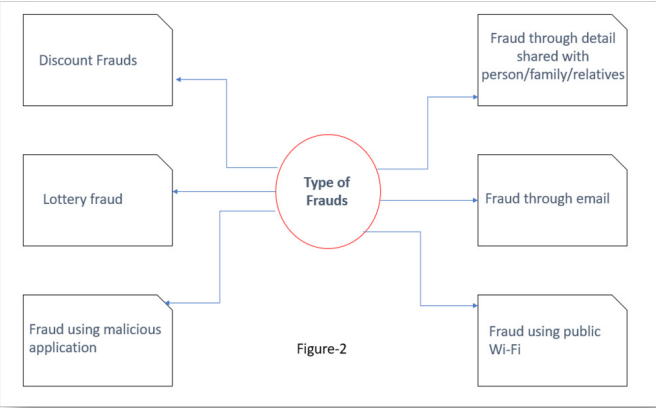

Figure 2: Types of fraud 2

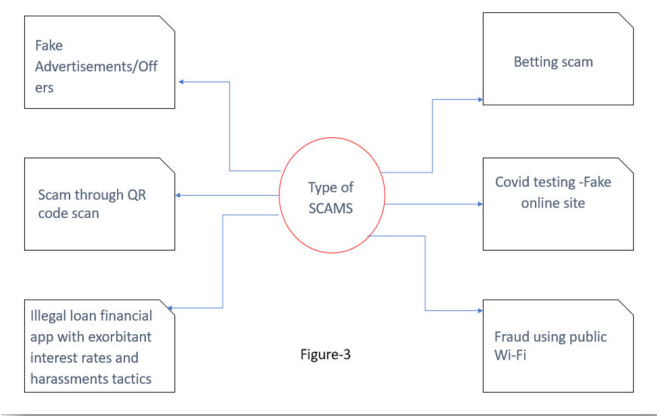

Figure 3: Types of scam 1

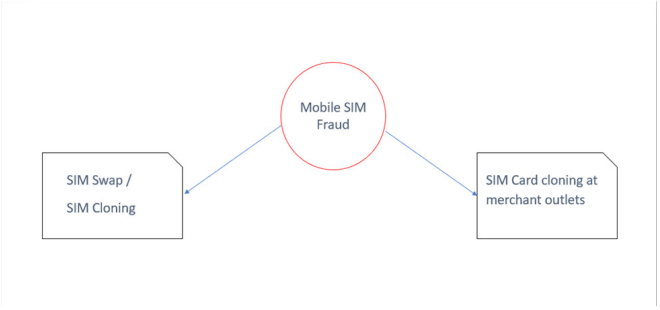

Figure 4: Types of fraud 3

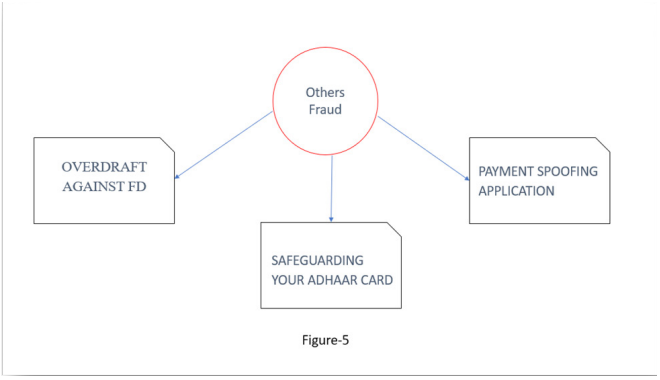

Figure 5: Types of other frauds

details in them to transfer the amount to particular account

- Do not download any application from unidentified / never click mysterious links receive on phone and e-mail without verifying it. Always verify the website details, especially where it requires entering financial credentials.
- One should be careful while making financial transactions for online goods and services
- Always remember that there are unverified sources.
- Ensure that there is no extra device attached near the card insertion slot while making transactions.
- Do NOT enter the PIN in the presence of any other person standing close to you or share the card with anyone, always cover the keypad with your hand while entering your PIN.
- Do not download or activate the share screen with unknown people
- Always remember that any Bank, financial institutions and any genuine entity never ask customers to share confidential information such as CVV/username / password / card details /OTP.
- If you do not have a mobile network on your phone for a considerable time in a regular environment, you should immediately contact Mobile operator to ensure that no duplicate SIM is being issued for your SIM
- Never share personal details/ OTP / PIN Number, in any form with anyone.
- Do not share confidential and secret information on social media platforms.
- Always verify the genuineness of the fund request with the friend or relative, physical meeting to ensure that the profile is not impersonated.
- Always remember that a genuine company offering a job will never ask for money. Do not make payments on unknown job portals.
- Never click on links sent through SMS / e-mails or reply to promotional SMS
- Never open/respond to e-mails from unknown sources containing suspicious attachments or phishing links.
- Never believe loan offers made by people on their own through telephones/e-mails etc.
- Never make any payment against such offers or share any personal/financial credentials against such offers without cross-checking that it is genuine through other sources
- If UPI or any other app asks you to enter PIN to complete a transaction, you will end up sending money instead of receiving it.
- Avoid searching for customer care contact details on search engines. Fraudsters often camouflage these. One should always look for official websites of Banks/ companies to get contact details
- Regularly check e-mails, sms to ensure that no OTP is generated without your knowledge.

Conclusion

In the above literature review, we show the most popular types of fraud. This study review can be an effective and efficient way to show the different fraud. The dangers of Internet handling are huge due to the variety of ways the information placed online can be altered. The alteration

of data in electronic commerce is another important area of Internet-related fraud. These data are subject to security frauds with several types of information misuse. All these areas of online fraud demand new preventive measures, such as governmental reforms, efficient data coding, and fraud avoidance strategies.

References

A.O., D. E., T.O., A., & A. J., O. (2017). Bank Fraud and Preventive Measures in Nigeria: An Empirical Review. *International Journal of Academic Research in Business and Social Sciences*, *7*(7). https://doi.org/10.6007/ijarbss/v7-i7/3076

Bănărescu, A. (2015). Detecting and Preventing Fraud with Data Analytics. *Procedia Economics and Finance*, *32*(15), 1827–1836. https://doi.org/10.1016/s2212-5671(15)01485-9

Baz, R., Samsudin, R. S., Che-Ahmad, A. B., & Popoola, O. M. J. (2016). Capability component of fraud and fraud prevention in the Saudi Arabian banking sector. *International Journal of Economics and Financial Issues*, *6*(4), 68–71.

Fraud Prevention and Detection. (2015). In *Computer-Aided Fraud Prevention and Detection* (pp. 17–39). https://doi.org/10.1002/9781119203971.ch2

Indrajani, Prabowo, H., & Meyliana. (2016). Learning fraud detection from big data in online banking transactions: A systematic literature review. *Journal of Telecommunication, Electronic and Computer Engineering*, *8*(3), 127–131.

Mining, D., & Detection, F. (2013). Big Data and Specific Analysis Methods for Insurance Fraud Detection. *Database Systems Journal*, *4*(4), 30–39. http://dbjournal.ro/archive/14/14_4.pdf

Ngigi Nyakarimi, S., Nduati Kariuki, S., & 'ombe Kariuki, P. W. (2020). Risk Assessment and Fraud Prevention in Banking Sector. *The Journal of Social Sciences Research*, *6*(61), 13–20. https://doi.org/10.32861/jssr.61.13.20

Patil, S., Nemade, V., & Soni, P. K. (2018). Predictive Modelling for Credit Card Fraud Detection Using Data Analytics. *Procedia Computer Science*, *132*, 385–395. https://doi.org/10.1016/j.procs.2018.05.199S1877050918309347. (n.d.).

State, O. (2021). *Of management research*. *3*(1), 91–99.

Ushmani, A. (2019). Internet Fraud Analysis. *International Journal of Computer Science Trends and Technology (IJCST)*, *7*(1). www.ijcstjournal.org