International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Risk Analysis in Online Banking Systems

Kanishka Deshmukh

Student, Abhinav Education Society's Junior College

Abstract
The rise of online banking has brought significant convenience but also heightened risks of fraud. This paper explores the evolving landscape of cyber threats targeting online financial transactions. It examines various forms of fraud, including identity theft, phishing, and malware attacks, and discusses advanced detection techniques such as AI-powered predictive analytics and machine learning algorithms. The study highlights the importance of multi-layered security measures and provides a comprehensive analysis of how financial institutions can mitigate these risks. The findings contribute to a deeper understanding of cybersecurity strategies and their implementation in the banking sector.

Keywords: Cybersecurity, Online Banking, Risk Mitigation, Cyber Threats, Encryption, Multi-Factor Authentication, Financial Institutions, Fraud Detection, Risk Analysis, Online Banking.

Introduction

In the Internet banking system, fraud refers to a lot of malicious activities. These activities are intended with the main aim of accessing unauthorized financial data of other people or gaining funds from it and more. The Internet banking system is surrounded by the risk of fraud.
In general, fraud can take place in various forms. Forms such as -Identity theft, Phishing, malware attacks, account takeover, card skimming, Social Engineering, and many more continue. As stated by Thomas Nagunwa in his 2014 International journal "Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors", states that the ever-changing landscape of phishing attacks, shedding light on how cybercriminals are staying ahead in this multi-billion-dollar cybercrime industry. It notes a decline in traditional phishing thanks to increased awareness and anti-spam technologies. However, hackers are countering with new, sophisticated tactics like spear phishing, malware, search engine poisoning, rogue SSL certificates, and mobile and social media attacks.
The study underscores the importance of comprehending these evolving strategies to develop effective technological, social, and legal defenses against phishing threats on a global scale. One key finding emphasizes that spear phishing serves as the gateway for most phishing attacks, with a particular focus on small and medium enterprises.

2 Which parameter defines which frauds in online banking in today's world?

Financial institutions employ a range of cybersecurity practices to protect online banking systems. On the other hand, the frauds mentioned above are increasing daily in the cybercrime industry. Let's delve into a fair- share idea of what the other frauds are –

2.1 Identity Theft

In simple terms, when the fraudster gains access to personal information such as your bank accounts, credit card numbers, etc. The fraudster further uses this information to impersonate and use it against the

victim. The fraudster can debit money from the victim's bank account at any given time in this case.

2.2 Malware Attacks

Generally, in this type of fraud, the fraudster can gain access to the victim's laptop or mobile device or any other personal devices using malicious software that provides the ability to hack into other's devices and gain access. Software such as key logger which records keystrokes or the infamous Trojan virus specifically designed to steal financial information.

2.3 Account Takeover

In this type of fraud, the fraudster gains access to one's online banking credentials. This usually happens because of stolen credentials or security weaknesses during the authentication process.

2.4 Card Skimming

These types of fraud are used worldwide; it is when the fraudster installs devices on the ATMs to capture card information. In online banking similar tactics are used to capture the card information while making payments or by recording the keystrokes of the victim.

3. Featuring Engineering Strategies for Improved Fraud Detection in Financial Transactions

If we look, in today's world keeping online banking transactions as secure as possible has become a necessity. As technology has evolved and advanced over the years, so do the methods used by fraudsters have increased deliberately. This section aims to explore the complexities and ways of fraud detection in online Internet banking by using diverse theories and methodologies. Our exploration is geared towards demystifying the complexities involved in securing digital financial interactions, explaining major important techniques into the adaptive strategies required to outsmart the evolving fraudulent practices..

- **An Insight**

Based on previous theories and methodologies, this area will discuss the pointers and techniques largely used to detect fraud. The method and theory used by Joh T.S. Quah and M. Sriganesh in their national research paper "Real Time Credit Card Fraud Detection using Computational Intelligence " in October 2007 - states that online banking and e-commerce have experienced rapid growth over the years. This rapid growth has made it easy for fraudsters to delve into new and complex ways of committing the 'Credit Card' fraud on the internet. The paper explains how an organization Map is used to decipher, analyze, interpret, and predict customer behavior and detect the possibilities of fraud on the internet system.

3.0 How frauds are prevented in Internet banking systems in today's world?

This section will explore the measures and solutions made by and used by a plethora of firms, organizations, banks, e-commerce, financial institutions, healthcare payments, Government bodies, cryptocurrency exchanges, traditional banks, etc.

Let's look into these measures more deeply to get a follow-up understanding of what is done to prevent fraud and stop fraudsters.

3.1 The Benford's Law in Audit

Advantage - The Benford's Law is used with MS Excel and IDEA software. It introduces the base of Benford's Law, its background history, and its application in detecting fraud. Benford's law has helped in identifying possible manipulation or misreporting of financial databases and its role in risk assessment for auditors.

Benford's law is also known as first-digit law. This law allows auditors to test 100% of the financial transactions and check for irregularities and possible manipulated data and fraud. Using MS Excel and IDEA software, auditors can perform compliance checks on datasets.

Overall, Benford's Law enables auditors to look through the transactions and access the datasets to check for any red flags in the transactions and potentially prevent frauds.

Disadvantage - On the other hand, when there are advantages, disadvantages follow. The limitation of Benford's Law is that certain specific conditions must be fulfilled for the law to work. Benford's Law may point out the occurrence of frauds in online transactions. It does not pinpoint the type of frauds occurred nor the nature of frauds which make it difficult to figure out. The data being analyzed must be of the same object i.e. lists of bad debts written off or population of cities.

3.2 Altman Z score Method -

An Altman Z score is a type score published by Edward I. Altman in 1968 as a Z score formula. This method is used to predict the possibilities and chances of a business to go bankrupt. This method is predominantly useful for evaluating risks for publicly traded manufacturing companies but over time it has been applied to other industries as well.

The Z score formula is as follows –

$Z = 1.2A + 1.4B + 3.3C + 0.6D + 1.0E$

The letter denominations are as presented below -

1. A = Working Capital / Total Assets
2. B = Retained Earnings / Total Assets
3. C = Earnings Before Interest and Taxes (EBIT) / Total Assets
4. D = Market Value of Equity / Total Liabilities
5. E = Sales / Total Assets

- **How are the results predicted?**

Well, the answer to that is simple –

- A score of 3 and above means that the company is in a safe zone and is unlikely to file for bankruptcy.
- A score lower than 1.8 means that the company is in financial distress and has a high probability of going bankrupt.

Limitations – Different industries have different affiliated benchmarks. Focusing on the primary intention of the Z score model is made for manufacturing companies. This model will not be useful for companies that have knowingly different financial structures. Financial circumstances change rapidly so the Z score model must be updated daily or must be monitored the whole time. The model depends on data that may not be available to private companies and thus the accuracy can be easily doubted for errors.

3.3 Two Factor Authentication (2FA)

In this type of prevention, the users are required to go through 2-step verification which indeed adds an extra layer of protection in online banking. This usually involves the user knowing the password and depending upon the use of this, the user generally gets a Time Password on his/her phone to verify the owner of the account. This helps in identifying the correct owner of the account and reduces the possibility of fraud taking place.

3.4 Device Recognition

While using Internet banking systems for any reason whether to make transactions on sending or receiving money or check balance, etc, many bodies have established device recognition systems in their websites and apps with the primary intention of tracking and recognizing devices used for online banking. This method is useful in internet systems as it also flags new or unrecognized devices for further authentication of the user.

3.5 Geolocation Tracking

This method has proved to be useful in identifying any fraudulent activities in online banking systems. In this method, the physical location of the user is detected and verified while making online transactions. By adopting this method one can detect potentially fraudulent activities if the transaction being made is from an unrecognized location. The geolocation information captured is factored into risk assessment for a better understanding of whether the transaction being made is safe or not.

3.6 AI-powered predictive analytics

The use of this method has increased significantly over the last few years. This method uses enormous amounts of data to make forecasts of future events, behaviors or drifts. The AI collects sundry data related to online Internet banking transactions and identifies sundry data, behavior, geological information, and other major factors. The system assesses real-time transactions and gives a score of the likelihood of fraudulent activities being conducted. Transactions with more likelihood of fraud are given more scrutiny and or more authentication processes. It can adapt to changing situations, analyze the data and give a prediction of future happenings.

The detailed intended analysis of Vaishnavi Nath Dornadula and Geetha S. states the use of machine learning in online banking systems in their national research article "Identification of Fraudulent Credit Card Transactions using Machine Learning Algorithms" published in 2019. The paper focuses on the increasing risk of online fraud because of the outpouring in online payment modes. The authors present a method for analyzing past transactions and detecting behavioral patterns. The research has used the drift and class imbalance in credit card transaction datasets. The process involves clustering cardholders recording their behavior patterns and smearing different fraud-detecting methods to the situation. The study also explains the use of the Matthews Correlation Coefficient (MCC) as a composed measure for evaluating the user's routine. Furthermore, the document deliberates the usage of SMOTE (Synthetic Minority Over-Sampling Technique) and one-class classifiers to discourse class imbalance in the dataset. The study revolves around 284000 transactions with a small percentage of them being fraudulent. The investigational results overall validate the efficiency of the projected methods in detecting fraud.

4. Association between fraud and risk

The evolution of online banking systems has improved the quality of online banking transactions and foremost accessibility for users. However, such convenience comes with certain inconveniences such as fraud and the risk of loss. In this discussion, we will dive into the key relationship between fraud and risk in the realm of online banking transactions. Distinguishing the perilous need for security against fraud, financial institutions are working their way up to making their sites more secure.

4.1 In Cybersecurity

As technology has advanced over the years so do the methods used by cybercriminals for conducting frauds. Financial Institutions must contend with the growing threats to secure their banking system. Threats such as Phishing, Malware attacks, etc.

4.2 Data Susceptibility

In the online banking world, data susceptibility is a growing concern as it exposes personal financial credentials to the fraudster hence increasing the possibility of fraud. There are several reasons for data exposure such as frail authentication, data fissures, third-party risks, and rarely insider threats.

4.3 Banking transaction encounters

In the world of online banking, various threats arise when it comes to online banking transfers such as

unauthorized fund transmissions, identity theft, account takeovers, Manipulation of transaction data, etc. Such great threats to online banking can cause a serious problem in future events if not taken care of. Financial Institutions are working hard to prevent fraud and increase online security systems for prevention.

5. How are these frauds assessed?

Well, the answer to the above questions is quite explanatory. There are some more techniques to assess these fraudulent activities and henceforth prevent them. Activities such as encryption technology, employee training, monitoring and incident response, customer education and awareness, and customer complaints and reports. Now, let's delve into these measures adopted by major and several major financial institutions and how it has affected the possibilities of fraud over time.

5.1 Encryption Technology

Applying encryption protocols to online banking systems such as 'end-to-end encryption' safeguards that the data remains safe at all costs and that no fraudulent activities can take place.

5.2 Employee Training

Training the employees on the importance of security in online banking is a crucial measure when it comes to the assessment of fraud. Training employees on security practices and the importance of sensitive information can help diminish insider threats and help guarantee an ethos of security in society.

5.3 Monitoring and incident response

Smearing real-time monitoring and incident response systems permit swift fraud detection and response and assess any apprehensive activities or security cracks. In this type of measure, usually, any anomalies or suspicious patterns can be easily detected and assessed for further authentication and verification of the user. Once a possible security event is detected and concluded through monitoring, the incident response lineups work to authenticate the incident's rationality. This usually involves analyzing alerts, logs, and other data to govern whether a security event has occurred.

Summary & Conclusion

Overall, this paper discusses the understanding of the factors involved in fraud detection in the realm of online banking systems in today's world, types of fraud, the definition of fraud, its association with risk, fraud models, methods of detection, and how these frauds are assessed.

This article gives a comprehensive analysis of how frauds surround online banking transactions and how financial institutions all around the world are working hard to prevent the event of fraud and to secure their customers from such activities.

This paper also explains the detection techniques from different authors and their references. It discusses how online banking systems must be protected by the given measure and by techniques to detect fraudsters and reduce the possibility of such drastic happenings.

This paper also refers to the works of different global authors around the world and how their methodology is practiced within contemporary society. In the end, this effort proposes a thorough analysis that accommodates a broad audience, encircling researchers, industry specialists, and individuals keen on stimulating the security of online financial transactions.

Works Cited

1. Pg 2 - Thoman Nagunwa

2. Nagunwa, Thoman, editor. "Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors." *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(1): 72-83 72 The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)*, vol. \, no. Cyber security threats, 2014, p. 12. *PDF*, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4c49e591bf6679f9430e1b8d038c18f9a871ae03.
3. Pg - 4 - Jon T.S. Quah, M. Sriganesh
4. Quah, Jon T.S., and M. Sriganesh. "Real-time credit card fraud detection using computational intelligence." *Expert Systems with Applications*, vol. 35, no. 4, 2008, \. *Elsevier*, https://www.sciencedirect.com/science/article/abs/pii/S0957417407003995?via%3Dihub.
5. Pg - 9 Vaishnavi Nath Dornadula , S Geetha
6. Dornadula, Vaishna Nath, and S. Geetha. "Credit Card Fraud Detection using Machine Learning Algorithms." *Procedia Computer Science*, vol. 165, no. -, 2019, p. 10. *Elsevier*, https://www.sciencedirect.com/science/article/pii/S187705092030065X.