JOURNAL OF APPLIED INTELLIGENT SYSTEMS & INFORMATION SCIENCES
VOL. 2, ISSUE 2, PP. 58-68, DECEMBER 2021.
Available at: **www.journal.research.fanap.com**
DOI: https://doi.org/10.22034/JAISIS.2021.319773.1040

BANKING FRAUD: A CUSTOMER-SIDE OVERVIEW OF CATEGORIES AND FRAMEWORKS OF DETECTION AND PREVENTION

Maghsoud Amiri [1], Siavash Hekmat [2, *]

[1] *Department of Industrial Management, Faculty of Management and Accounting, Allameh Tabataba'i University, Tehran, Iran*
[2] *Faculty of Industrial and Mechanical Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran*

ABSTRACT

Online banking and digital payments are among the most fundamental solutions offered within the present-day banking system to simplify the usage of financial services for businesses or individual customers. The pivotal role of these solutions in today business makes them equally favorable for end-users and for cyber-criminals. It is no secret that reputational risk mitigation besides regulatory compliance have always been among the first priorities of banking and financial institutions. Hence, detection and prevention of fraudulent activities are crucial for both customers and institutions in banking industry. The importance of banking fraud, compared to the well-known research title of financial fraud, becomes more obvious when it is studied as a topic that has rarely been discussed before. This study, based on an initial categorization of banking fraudulent activities according to the literature, intends to provide an overview of existing fraud detection and prevention frameworks from a customer-side point of view. Hence, six categories of banking fraud are identifiable. Challenges of fraud detection in operational environments, and behavioral and technical prevention approaches are the other subjects to be explored in the paper. Anomaly detection, artificial intelligence, and machine learning are some key prevention approaches to be discussed here.

KEYWORDS: fraud detection, fraud prevention, financial fraud, online banking, phishing.

1. INTRODUCTION

In the past decade, digital payments have been improving significantly (Crowe et al., 2019). The US based Zelle digital payment service processed 743 million transactions (with the value of 187 billion USD) in 2019. This means that the total transaction amounts have experienced a 57% year-to-year growth and the transaction volumes have increased by 72% (Scottsdale, 2020). In china, mobile payments increased by more than 120% in only 6 years from 2013 to 2018 (Bansal et al., 2019), and likewise this volume grew by 61% in India during the past 5 years.

The opportunity to access financial services has been provided for many individuals across the world by mobile banking and digital payments. Hence, many valuable benefits such as time-effectiveness, cost-effectiveness, speed, and ease of use have been offered to the individual consumers, businesses, and financial service providers through these opportunities (Kurshan et al., 2020).

[*] *Corresponding Author, Email: siavashhekmat@gmail.com*

RECEIVED: 14 NOVEMBER, 2021; ACCEPTED: 25 DECEMBER, 2021; PUBLISHED ONLINE: 28 DECEMBER, 2021

The security issues encountered in information systems or networks are the unavoidable part of them. By abusing this theme, hackers can break right into financial systems in various ways. As a result, in order to guarantee a secure communication over such systems, networks need to be protected by service providers against various kinds of online attacks (Taha et al., 2019).

The significant internet growth has offered noticeable advantages to the business environment (including the e-banking industry). By offering noticeable customer-related benefits as well as new business platforms for banks, e-banking revolutionized the banking business. Nevertheless, challenges such as banking risks, and security issues are the unavoidable consequences of such a revolutionary technology. Financial organizations need to take into account the security aspects at all levels to prevent different forms of fraud (Ali et al., 2019).

As an introductory definition, fraud is articulated in academic texts as any behavior that aims at gaining a dishonest advantage over another person by a way of concealing facts (Chakrabarty, 2013). Banking fraud is mostly committed by electronic gateway attackers who illegally try to exploit vulnerabilities and confront customers with financial service denial (Ali et al., 2019; Weinflash et al., 2018).

The most recent industry reports have indicated that financial crime volume across the world is around 1.4-3.5 trillion USD annually (Piper & Metcalfe, 2020). According to other sources money laundering is about 2-5% of the global GDP (up to 1.87 trillion EU), many of which remains undetected (Shepard et al., 2019). The U.S. Federal Trade Commission (FTC) reported 3.2 million fraud records in 2019 alone; and this demonstrates a 53% increase from 2018 (Kurshan & Shen, 2020).

Recently significant changes have been applied to financial crime schemes. The recent industry surveys indicate that almost all fraud types have undergone serious increases (Hicks et al., 2019). The rise in external fraud, both in terms of volume and total transaction, amounts by 61% and 59% respectively (Kurshan et al., 2020).

Financial crime tactics are always highly adapted to the emerging digital or online devices, platforms, and the pertinent cybersecurity-threats. Parallelly, this issue has yielded to the enhanced efficiency of fraud detection mechanisms. The correctness of this occurrence is evident in the rise of identity theft and account takeover (ATO) fraud and decline in in-person credit card fraud (Kurshan & Shen, 2020).

Organizations in critical sectors such as government, energy, healthcare, banks, and research centers have found that monitoring the networking threats is the most serious challenge and thus made large investments on various monitoring tools to guard and secure the infrastructure. However, since hackers utilize complicated techniques to break into the infrastructure, the existing security tools and analysis of logs used to detect the attackers in offline mode wear out in the long run and become obsolete (Habeeb et al., 2019).

The new fast-moving digital payments landscape has benefited many criminal schemes. Traditionally, in order to flag suspicious transactions, a large number of rules and static thresholds (e.g. in transactions of $10,000 and more) were used in the process of crime detection. However since fraudsters find out these rules immediately and avoid them, recently these manual and rule-based techniques have become insufficient (Kurshan et al., 2020).

The negative effects of financial crimes on a country’s welfare through macroeconomic performance are an example of how these crimes might affect individuals and financial institutions. Recently, the interest in artificial intelligence (AI) and machine learning (ML) solutions have increased significantly in the financial services industry in terms of compliance and risk management functions (McWaters & Galaski, 2018). Graph algorithms and databases have long been considered as important tools in fraud detection (Buehler, 2019). Utilizing anomaly detection, network flow and sub-graph based analysis proved to be effective according to many researches (Phua et al., 2010). Graph neural networks have become popular recently (Gori et al., 2005). These networks have been deployed in many industries before the financial services applications (Kurshan & Shen, 2020).

Payment fraud detection systems have utilized AI and ML models extensively (Buehler, 2019) since the 1990s (Piper & Metcalfe, 2020; Scottsdale, 2020). Lately, the unprecedented increase in the digital payments has caused major challenges for fraud detection. Global payment fraud losses are estimated to be well over 25 billion USD per year (Bansal et al., 2019; Phua et al., 2010). Financial institutions have spent large amounts of money on upgrading and building in-house AI models in response to these losses. Models such as supervised (Gottschalk, 2010; Zhou et al., 2020), semi-supervised and unsupervised learning (Scottsdale, 2020), deep neural networks, decision trees (Morgan, 2020) and hybrid approaches have been widely studied for deployment in fraud detection systems. However, transaction fraud scoring has been the focus of AI and ML applications in fraud detection. Yet, rule-based or manual processing stages are still being utilized by many downstream systems which still have limited AI modeling (Shen & Kurshan, 2020).

Based on the review of former studies, authors of this paper came into the conclusion that banking fraud is a subject which is rarely discussed so far. Additionally, it is resulted that all types of financial fraud are investigable from both institution-side and customer-side individually. Hence, this study is conducted from a customer-side point of view as a novel approach. This research, apart from its academic value in summarizing the former studies, is appliable as a security guide for analyzing or developing banking software or in-person services. On the mentioned basis which is considerable as the contribution of the present study, the remaining of this paper is organized as follows: Next, different categories of banking fraud are explored. Detection pattern and framework of banking fraud is another subject which is considered in section 3. In section 4, banking fraud prevention options are stated, and the concluding remarks are explained in section 5.

2. Categories of Banking Fraud

The literature of financial crime types and trends is replete with various categorization schemes. Gottschalk (2010) believes that there are four main categories in financial crime which include: corruption, fraud, theft, and manipulation. Kickbacks, bribery, extortion, and embezzlement are different types of corruption crime which are connected to institution-side issues and are not investigable within the scope of current study. However, the main customer-side banking crime types occur within the last three mentioned categories of financial crime. Hence, the following categorization is considerable for banking fraud types according to Fig. 1 based on Kurshan & Shen (2020), Kurshan et al. (2020), Ali et al. (2019), and other researches in the literature.

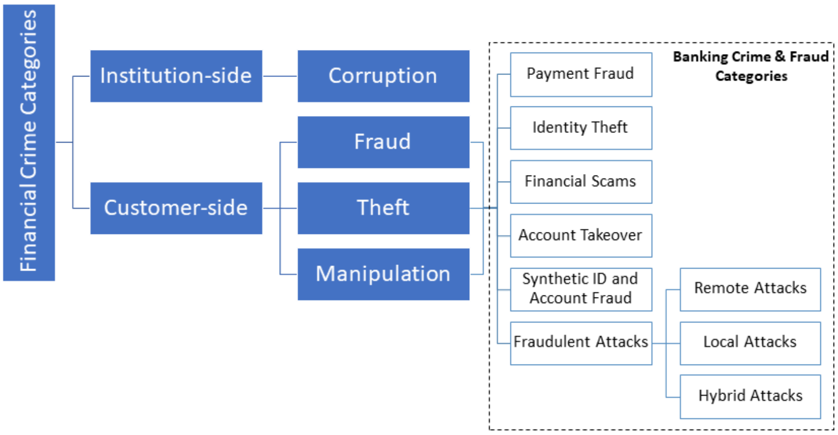

Fig. 1. Financial crime categories and banking fraud subcategories

2.1. Payment Fraud

This fraud type is involved with criminal activities which are conducted in numerous payment channels. Transactions ranging from card-present (CP) to card-not-present (CNP) in these channels are mainly related to credit and debit card payments. Point of sale (POS) and automated teller machine (ATM) channels chiefly operate CP transactions. In contrast, online procedures including internet payment gateway (IPG), automated bill payment, person-to-person (P2P) payment, automated clearing house, and payments via checks or deposits are where CNP transactions get processed. The increase in recent fraud and money laundering activities through CNP channels is mainly caused by the popularity and noticeable usage of online and mobile payment channels.

While Morgan (2020) announced that payment fraud is currently reported at over 80% of organizations and is still in the rise, the European Central Bank considers card fraud, including credit and debit card fraud with losses reaching to 1.8 billion EUR in 2016, as one of the largest segments in payments fraud (ECBank, 2019). Chip cards and personal identification number (PIN) usage has caused shifts in the fraud tactics from CP to CNP transactions. CNP fraud is still on the rise and it increased to more than 70% of the total card fraud in spite of introducing new approaches such as 3D-Secure.

As mentioned above, there has been a noticeable growth in all online payment channels recently (from bill payments to P2P and online check processing). Frequent crossovers among payment channels and fraud types are reported in this regard. An example of this relates to the World Bank reports which demonstrate that mobile payment channels are progressively used by criminals for money laundering (Chatain et al., 2011). Financial crime organizations continuously intend to conduct large merchant hacks to have access to card-related information of tens or hundreds of millions of accounts as a result of their tendency to achieve economies of scale (Kurshan & Shen, 2020; Sullivan, 2010).

2.2. *Identity Theft*

The act of stealing an individual's personal information in order to conduct a fraud is called Identity theft. A dynamic list of tactics varying from ATM skimming devices to phishing, smishing, dumpster diving, and compromised wireless networks are utilized in ID theft schemes. After criminals commit an identity theft, they usually utilize the compromised information across multiple channels. In comparison to the other financial fraud types, identity theft and new account frauds cause more financial damage and that is because of the time it takes to detect them. As Newman and McNally (2005) reported, close to 58% of the ID theft cases are discovered after 4 months and even approximately 25% of the cases are discovered after 2 years. The financial crime organizations find these long discovery periods to their benefits and thus they become motivated to further invests in ID theft schemes (Kurshan et al., 2020).

2.3. *Financial Scams*

An extensive range of fraud and criminal activities, which utilizes deception as a means to steal from targeted individuals, is called financial scam. Evolving tactics such as phone scams, technical support scams, elderly scams, charity and lottery scams, and ticket scams are repeatedly utilized in these crimes. Each of these tactics comprises a long list of approaches. As an example, customized elderly scams include insurance scams, internal revenue service (IRS) impersonation scams, mortgage scams, and grandparent scams (Deane, 2018).

Recently, this type of fraud focuses on the elderly people because of the increase in their population. Moreover, financial scams, which have become one of the major fraud issues, are in close relation with identity theft, account takeover, and their downstream fraud tactics within multiple channels. Detecting financial scams and the downstream fraud cases can be efficiently achieved through analysis of interconnectivity as well as the shared network patterns.

2.4. *Account Takeover*

Account takeover occurs when a cyber-criminal tries to access the customers' credentials and their authentication methodology by signing into the online banking platforms, resulting to the electronic stealing of funds (Examining Faster Payments Fraud Prevention, 2020). In order to prevent the victim from gaining access to the account, fraudsters change the login credentials and contact information during ATO. They eventually withdraw the funds through one or more payment channels. Since the criminals utilize different cyber approaches for their attacks, ATO is tightly related to cybersecurity. The approaches include mass data breaches, mobile SIM hijacking, and vulnerabilities of devices and networks. A key role is hence played here by improved authentication technologies, end-point security, and other cybersecurity practices (Moore, 2010). Similar to identity theft, ATO offers a gateway to numerous downstream fraud types.

ATO begins by a cyber-criminal using various methodologies to steer victims into disclosing information which are required eventually to gain access to an online banking account. The various methodologies may include opening a malicious email attachment, accepting friend/follower requests on social media or networking accounts, or visiting websites – even legitimate websites – which may then install malware onto the user's computer. Infecting the user's computer with the malware utilized to scan the users' activities, such as checking a financial institution's website as well as entering login credentials, is the ultimate goal of the cyber-criminal. After the cyber-criminal get access to the information, they can use the user's own login credentials and commit unauthorized transactions (Examining Faster Payments Fraud Prevention, 2020).

Lately, there has been rapid changes in the crime topologies and the channels through which criminals commit the crime (Castell, 2013). Financial crimes, fraud, and cybersecurity threats are rapidly converging (Hasham et al., 2019). ATO gives a good example of this convergence which challenges the detection process of criminal activity. Cybercrime tactics like spear-phishing, back-doors, infected devices, ATM hacks, and balance alterations have become progressively noticeable in financial services attacks. The defense mechanisms of traditional financial services are hence weakened as a result of their inefficiency in dealing with recent changes. On the other hand, because the financial crime organizations commit repetitive attacks to find efficiency, ample opportunities are developed through the integration of cyber-defenses with financial crime detection techniques. Graph-based techniques are the typical outcome of this integration.

2.5. *Synthetic ID and Account Fraud*

Forged identities that look like customers with desirable credit scores and characteristics form the basis for synthetic account fraud. Social security numbers and credit privacy numbers integrated with real and synthetic information from one or more individuals are usually used by Synthetic ID fraud cases.

Recently, the synthetic ID and account fraud has been growing significantly. The non-transactional nature of synthetic ID/account fraud is the main reason for this trend. Thus, discovering it takes longer and it lacks the traditional crime reporting paths used by other fraud types (e.g., reporting fraudulent credit card transactions). Hence, the longer time-to-discovery leads to proportionally higher obtained financial gains.

Synthetic identity fraud is the fastest growing type of financial crime in the United States according to the estimates of the Federal Reserve. However, detecting the synthetic identity fraud is complex. The victims in this kind of fraud are usually children, the elderly, or the homeless who have less access to their credit information. Hence, this type of fraud often goes unreported. The gaps in the credit process and the potential for large payouts have made the synthetic ID fraud popular among the criminals. Incompatibility of the definitions with detection approaches make synthetic identity payments fraud barely measurable according to industry experts (Payments Fraud Insights: Synthetic Identity Fraud in the U.S. Payment System, 2019).

2.6. *Fraudulent Attacks*

Hackers can commit attacks in various ways. However, the critical issues the information systems experience today are inherent within the computer systems and communication networks. Remote, local, and hybrid groups are the different classes of the various forms of attacks in the literature. Next, the mentioned attack types are discussed based on Ali et al. (2019).

2.7. *Remote Attacks*

The reason behind the remote attack is to interrupt or redirect a systems' session without modifying the victim machine. The common types of remote attack are explained next.

i) Phishing: It takes place when a hacker sets up a fabricated version of the targeted website. The impersonated website version may have all the codes and the user interface of the original website. The fabricated website is then utilized by the hacker to send messages to several email accounts in order to manipulate the message recipient into visiting the spoofed website and reveal their logon details (Brar et al., 2012). Phishing attacks might include personalized messages, properly formatted hyperlinks, and similar branding (Examining Faster Payments Fraud Prevention, 2020).

ii) Fishing: This takes place when a hacker uses social engineering in order to contact the victim and to trick them into revealing secret information (Brar et al., 2012).

iii) Smishing: This is an SMS (text message) version of a phishing cyber-attack. SMS is used instead of email template by the criminals to trick recipients into divulging credentials via text message reply. Because people are more cautious about the phishing attacks, attackers sometimes resort to this new technique. Users' trust in SMS is a major factor on which scammers rely to manipulate people into revealing sensitive data, including banking details and credit card details.

iv) Vishing: This is the voice version of phishing which utilizes voice messages in order to steal identities and financial resources. A relevant research indicates that malicious voicemail messages are not just increasing but are evolving and are more nuanced than ever before (Examining Faster Payments Fraud Prevention, 2020).

v) Cloned voice-banking systems: In this situation a hacker clones the voice-banking system to make it sound like the official system. This attack uses fake e-mails to solicit customer calls to a fake phone number (Brar et al., 2012).

vi) Pretexting: This is a remote attack type based on social engineering which uses a fictional backstory in order to trick people into giving up private information or to influence their behavior. Generally, the fraudster uses the story or pretext to get access to financial or authentication information. For example, a scammer might report a device lost and ask the mobile provider to activate a new SIM card for the victim's phone number. If a customer service agent believes the criminal, the victim's phone number gets activated on the criminal's device. Now the criminal can circumvent two-factor authentication via SMS or voice calls to that phone. In addition, many scammers use current events as a hook or pretext to perpetuate the fraud (Examining Faster Payments Fraud Prevention, 2020).

2.7.1. *Local Attacks*

Local attacks might occur in websites where only a fake password request is offered. Indeed, the fake request includes a malicious intent that is not part of the original website. Even the secure sockets layer (SSL) padlock might divulge the correct certificate details and the URL in the address bar is not spoofed here.

There is one other type of local attacks named shoulder surfing which occurs when the hacker monitors the PIN of a bank card before the physical card is actually stolen (Brar et al., 2012).

2.7.2. *Hybrid Attacks*

Merging the features of both local and remote attacks, hybrid attacks are among the fiercest types of attack. The hacker in this situation never limits himself to only one type of attack. In these attacks, a Trojan is executed on the affected machine. This is achieved by examining all bookmarked pages and replacing important online service addresses with fake ones. Moreover, the browser setting might be modified in order to guarantee that the address bar is not displayed or is overlaid with a fake pop-up window to hide the modified URL from the user. Usually, the attacker makes sure that he has utilized the system to its full capacity and could even change the host files or redirect certain domains to a set IP address (Brar et al., 2012).

3. Banking Fraud Detection

Extraordinary levels of customization to the individual channels and the multi-channel modes are achieved by the fraud tactics. Significant changes in the characteristics of fraud are displayed in different channels: differences such as transaction type, amounts, processing times, devices, authentication requirements, etc. Take ATM fraud as an example which is significantly different from online bill payment fraud in terms of frequency, amounts, transaction and processing time-ranges, parties involved, access compromises, devices involved, etc. Such unique characteristics have a major role in the efficiency of the algorithmic solutions. Usually, these differences lead to different performance levels: for example, the techniques that mostly perform well in one channel become challenging in others due to difference in the environment dynamism, scale, attributes, etc. Furthermore, another challenge exists in balancing the channel-specific patterns with the need to integrate the techniques for multi-channel fraud (Kurshan et al., 2020).

Utilizing the internet and digital platforms has turned the nature of financial fraud into a cross-border and transnational state, as Interpol announced. Financial crime organizations are not only able to hide the identities over diverse geographical footprints, but they can also rely on complex transaction patterns and diversified geographical operations. The criminal organizations can also transfer unauthorized money to locations with low security through transnational fraud. Hence, although online fraud is still a major issue, AI and ML solutions such as graph-computing offer remarkable benefits leading to the achievement of interconnectivity-based analyses at the global scale (Kurshan & Shen, 2020).

Based on a published research on online banking fraud, it is concluded that most of banks have the following fraud detection challenges (Ali et al., 2019; Wei et al., 2013):

- Highly imbalanced large dataset: What turns the fraud detection into a serious challenge is the large number of daily online transactions conducted on the e-banking platforms containing relatively small number of the daily frauds.
- Real-time detection: In order to guard against the instant financial losses, fraud detection needs to be conducted in real-time in online systems.
- Dynamic fraud behavior: To avoid online banking defense systems, criminals continuously change their tactics. These thriving set of online attacks cannot be prevented through a simple detection system.
- Weak forensic evidence: Forensic evidence corresponding with each e-banking transaction is required in order to find out the nature of fraudulent behaviors.
- Diverse behavioral customer patterns: Since different types of online banking transactions are performed in different ways by customers, there is an increase in the number of actual transactions which can be simulated by the criminals. This is the reason why it is hard to differentiate fraudulent behaviors from genuine ones.

3.1. Fraud Detection Framework

The existing online fraud detection methods are rule-based as they involve the generation of rules based on the domain knowledge. As a result, there is usually a high level of false alarm rate in these systems (too many false positive situations), meaning that the fraud detection rate is low. A general fraud detector framework was proposed in former studies with the following main issues (Ali et al., 2019; Kovach & Ruggiero, 2011):

- Device identification: A downloadable component used by the real online banking system helps to identify the access device. This component generates the access devices' fingerprint which is sent to the bank website as a part of every transaction.
- Monitoring the global behaviors: Here, the fraud is detected by monitoring a user's global behavior. For example, in order to detect a fraud, all the accounts that are accessed through a single device may be monitored. Moreover, all login failures over different accounts using a single trial password may be monitored. The monitor process also utilizes counters to check updated transactions.
- Deferential analysis: Here, a comparison is made between all incoming transaction requests against a set of profiles that show the normal usage patterns. Hence, the unordinary deviations might reveal fraudulent behaviors. Password failures, payment transaction frequency, and login frequency are behaviors that often used in differential analysis.
- Global analysis: The fraud evidence already specified by the differential analysis might underestimate or overestimate. In order to determine the occurrence probability of this evidence three lists are used: blacklist (contains the fraudulent identities), white list (contains the legitimate identities), and the suspect list (contains unclassified identities).
- Suspect list and the exponentially decaying function: Before specifying the fraud likelihood, devices are assigned into one of the three lists following specific rules. A suspected device has an initial assigned value for the probability of fraud, calculated using a rapidly decreasing function related to the number

of accounts accessed by the device. The identity of the related device is placed in the blacklist in case a customer reports any of these accounts as a fraud account.

- Dempster-Shafer combiner: This refers to the mathematical theory of fraud evidence based on combining different sources of evidence estimated by global and differential analysis modules. This combiner is employed with the purpose of computing a transactions' overall suspicion score.

4. Banking Fraud Prevention

In order to guard against fraud, efficient security models are required. These models can identify users and authorize transactions. Now, the current models focus primarily on fraud detection rather than its prevention. This means necessary measures are often taken after the fraud is committed and there is no system in place preventing it from occurring (Ali et al., 2019; Peotta et al., 2011).

Security actions taken with the purpose of preventing unauthorized access or transaction initiation is called fraud prevention (Bolton & Hand, 2002). A list of technical and behavioral controls for fraud mitigation is presented in this section. The list includes both behavioral and processing practices and concentrates on activities a consumer or organization can conduct. Many approaches apply equally to all digital channels related to mobile devices or web. Mobile devices including tablets and smartphones are becoming very common. They are popular because of their mobility and size, however, these benefits come with some disadvantages as well. For instance, a smartphone is quite more probable to be stolen or lost than a personal computer (Examining Faster Payments Fraud Prevention, 2020).

In an attempt to improve the security of the domestic banking systems, accomplish public trust, and defend consumer rights, many national regulators not only applied the methods used for fraud prevention in online platforms, but they also strengthened their regulations. Licensing, individuals' identity verification, capacity planning, legalization, harmonization, adaptation, and integration are some of the policies that can guarantee a safe and secure online banking ecosystem (Ali et al., 2019; Bahl, 2012).

In the following, some options for fraud prevention are presented. It should be noticed that some of these options are also regarded by some researchers as fraud detection techniques.

4.1. Behavioral Control

Information double-check: According to the best practices, double- and even triple-checking of the recipient information is necessary before sending money via any device or platform. This is particularly necessary to guarantee that the funds are transmitted to the intended individual or to an organizational receiver (Examining Faster Payments Fraud Prevention, 2020).

4.2. Technical Controls

Anomaly Detection using AI and ML: AI and ML are used by many payment providers in order to analyze and detect potentially fraudulent measures. In case an account measure does not comply to an expected behavior, an alert is sent by the anomaly detection system. ML utilizes a set of rules and updates its dataset repeatedly in order to learn about authorized and fraudulent transactions. This output is also used to update the rules and identify new trends. Instead of applying a standard ruleset to a group of accounts, each account has its own, unique profile based on ML (The AI innovation playbook: How FIs are using artificial intelligence and machine learning, 2019).

Behavioral Biometrics: Enabling physical biometric security features, such as fingerprint or facial recognition, helps in augmenting the existing protections. A human dimension is added to the authentication process by behavioral biometrics. The behavioral biometrics can also be used regularly in order to assess the authenticity of an established session, which can help in preventing criminals from using stolen credentials or in identifying bots (Wang & Geng, 2009).

Device Identification: Applicant devices, as having been previously authenticated with their payment devices, are identified by a ‘smart cookie’ in many financial institutions (Examining Faster Payments Fraud Prevention, 2020).

Knowledge-Based Authentication (KBA): KBA asks ‘shared secret’ questions that only the actual person should know to authenticate the end-users. Although some customers are allowed to design their own questions to make it difficult to guess the answer, anything known is potentially at risk of being inadvertently shared or stolen. (Examining Faster Payments Fraud Prevention, 2020).

Tokenization or Aliases in a Directory: Banking credentials are covered using this method most of time. In this process, the account numbers are substituted with either a token or associated with an email address or telephone number (Examining Faster Payments Fraud Prevention, 2020).

SMS Challenge Code: This is utilized to guarantee that a user logs on by receiving an activation code in a registered mobile phone corresponding to their bank account. Such temporary passwords are generated and sent as SMS to the user’s mobile phone number by the bank. To access their account, the users then utilize these passwords (Ali et al., 2019).

Dynamic Security Skins (DSS): Here, the user is required to choose an image that is overlaid on web forms. The chosen image includes a virtual hash and is tied to the secured SSL session. This prevents the criminals from spoofing a pop-up similar to password requests (Ali et al., 2019).

PKI-based Software Solution: Both the user and the server can be authenticated using the Public Key Infrastructure (PKI). ‘Man in the Middle’ attack would be prevented by this type of authentication (Ali et al., 2019).

PKI-based Hardware Token: This system uses tamper-resistant key storage to guarantee security against Trojans, which can steal PIN codes and private keys from a PKI-based software token. Thus, the certificates and key pairs are pre-generated and saved on a tamper-proof smartcard. In order to unlock the key vault in the smartcard and prevent key logger, PIN code on the external storage is used here (Ali et al., 2019).

5. CONCLUSION

With the advancement of technology, people across the globe connect to each other more rapidly. On the other hand, the improvement of connectivity has provided individuals and businesses with easier and more efficient transactional banking services. The convenience and higher speed of online and wireless payment options caused by technological enhancements is the other incentive for this happening. Nevertheless, these beneficial features have made new forms of criminal activities hard to detect and prosecute. In an attempt to detect, assess, control, and report the defects which can be abused by management, employees, vendors, or external criminals, companies tend to repeatedly evaluate and examine their information security standards, systems of internal control, policies, and procedures.

Fraud has always been a critical challenge in the payment industry. Hence, criminals are expected to manipulate any weaknesses in the ecosystem and take advantage of them. In this regard, the focus of the present study is placed upon two remarkable considerations including the approaches of being informed about fraudulent conducts, and the techniques to alleviate the related situations. In other words, fraud detection and fraud prevention are the two main issues investigated in the present research from a customer-side viewpoint. As a prerequisite to reach this goal, the investigation of banking fraud types and categories was considered in the paper prior to the mentioned issues.

Financial crime and fraud schemes have rapidly evolved to adapt to the new digital payments landscape. Within this scope, research and development is essential for competitiveness in financial industry. As a remarkable instance, research-based approaches are at the core of the ML revolution in terms of fraud detection techniques. However, in a situation where scholars only tend to elaborate on the research part of the process, the complete fraud detection and prevention path from emergence to deployment hides many other challenges.

A valuable milestone in this way is achieved when real time anomaly detection and fraud prevention approaches are deployed for large-scale financial systems utilizing cost-effective and reasonable hardware equipment.

REFERENCES

Ali, M., Hussin, N., & Abed, I. (2019). E-banking fraud detection: A short review. *Int. J. Innov. Creat. Chang, 6*(8), 67-87.

Bahl, S. (2012). E-banking: Challenges & policy implications. *International Journal of Computing & Business Research*, 229-6166.

Bansal, S., Bruno, P., Denecker, O., & Niederkorn, M. (2019). Global payments report 2019: Amid sustained growth, accelerating challenges demand bold actions. *McKinsey Global Payment Reports*.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical science, 17*(3), 235-255.

Brar, T., Sharma, D., & Khurmi, S. S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. *International Journal of Computing & Business Research*.

Brighterion & PYMNTS. (2019). The AI innovation playbook: How FIs are using artificial intelligence and machine learning.

Buehler, K. (2019). Transforming approaches to aml and financial crime. *McKinsey*.

Castell, M. (2013). *Mitigating online account takeovers: The case for education.* Paper presented at the Retail Payments Risk Forum Survey Paper.

Chakrabarty, K. (2013). *Fraud in the banking sector–causes, concerns and cures.* Paper presented at the National Conference on Financial Fraud organised by ASSOCHAM, New Delhi.

Chatain, P.-L., Zerzan, A., Noor, W., Dannaoui, N., & De Koker, L. (2011). *Protecting mobile money against financial crimes: Global policy challenges and solutions*: World Bank Publications.

Crowe, M., McGuire, B., & Tavilla, E. (2019). Financial institutions across the us participate in the mobile landscape transformation. *Federal Reserve Bank of Boston*.

Deane, S. (2018). Elder financial exploitation: Why it is a concern, what regulators are doing about it and looking ahead. *Retrieved December, 10*, 2018.

ECBank. (2019). Fifth report on card fraud. *European Central Bank: Frankfurt am Main, Germany*.

Federal Reserve Banks. (2019). Payments Fraud Insights: Synthetic Identity Fraud in the U.S. Payment System.

Gori, M., Monfardini, G., & Scarselli, F. (2005). *A new model for learning in graph domains.* Paper presented at the Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005.

Gottschalk, P. (2010). Categories of financial crime. *Journal of financial crime*.

Habeeb, R. A. A., Nasaruddin, F., Gani, A., Hashem, I. A. T., Ahmed, E., & Imran, M. (2019). Real-time big data processing for anomaly detection: A survey. *International Journal of Information Management, 45*, 289-307.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*.

Hicks, D., Caplain, J., Faulkner, N., Olcina, E., Stanton, T., & Kok, L. (2019). Global banking fraud survey the multi-faceted threat of fraud: Are banks up to the challenge? *KPMG*.

Kovach, S., & Ruggiero, W. V. (2011). *Online banking fraud detection based on local and global behavior.* Paper presented at the Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France.

Kurshan, E., & Shen, H. (2020). Graph Computing for Financial Crime and Fraud Detection: Trends, Challenges and Outlook. *International Journal of Semantic Computing, 14*(04), 565-589.

Kurshan, E., Shen, H., & Yu, H. (2020). *Financial Crime & Fraud Detection Using Graph Computing: Application Considerations & Outlook.* Paper presented at the 2020 Second International Conference on Transdisciplinary AI (TransAI).

McWaters, J., & Galaski, R. (2018). *The New Physics of Financial Services: Understanding how artificial intelligence is transforming the financial ecosystem.* Paper presented at the World Economic Forum.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3-4), 103-117.

Morgan, J. (2020). Payments fraud and control survey report.

Newman, G. R., & McNally, M. M. (2005). Identity theft literature review.

Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., & de Sousa, R. T. (2011). A formal classification of internet banking attacks and vulnerabilities. *International Journal of Computer Science & Information Technology, 3*(1), 186-197.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv:1009.6119*.

Piper, J., & Metcalfe, A. (2020). Economic crime in a digital age. *Ernst & Young Report*.

Scottsdale, A. (2020). Gift giving helps zelle wrap up 2019 with double digit growth [Press release]

Shen, H., & Kurshan, E. (2020). Deep Q-network-based adaptive alert threshold selection policy for payment fraud systems in retail banking. *arXiv preprint arXiv:2010.11062*.

Shepard, M., Adams, T., Portilla, A., Ekberg, M., Wainwright, R., Jackson, K., . . . Lagoss, P. (2019). The global framework for fighting financial crime enhancing effectiveness & improving outcomes. *Deloitte Report*.

Siblini, W., Coter, G., Fabry, R., He-Guelton, L., Oblé, F., Lebichot, B., . . . Bontempi, G. (2021). Transfer learning for credit card fraud detection: A journey from research to production. *arXiv preprint arXiv:2107.09323*.

Sullivan, R. J. (2010). *The Changing Nature of US Card Payment Fraud: Issues for Industry and Public Policy.* Paper presented at the WEIS.

Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). *Combination of steganography and cryptography: A short survey.* Paper presented at the IOP conference series: materials science and engineering.

U.S. Faster Payments Council. (2020). Examining Faster Payments Fraud Prevention.

Wang, L., & Geng, X. (2009). *Behavioral Biometrics for Human Identification: Intelligent Applications*: IGI Global.

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web, 16*(4), 449-475.

Weinflash, L. E., Simm, J. E., & Qi, J. (2018). System and method for detecting fraudulent account access and transfers: Google Patents.

Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., . . . Sun, M. (2020). Graph neural networks: A review of methods and applications. *AI Open*, *1*, 57-81.