

A Systematic Review On Identification And Mitigation Of Frauds In Banking Sectors

Swati Srivastava , Dr. Roheet Bhatnagar

Abstract: -

Banks are vital to a country's economy, helping both citizens and governments. Many fraudulent bank transactions have been discovered in recent years as a result of entrenched interests. This study explores and attempts to categorise the most typical types of insider fraud that occur in banks. This page includes a description, variables related with certain types of fraud, and obstacles in identifying frauds. It is vital to automatically detect such fraudulent occurrences before it is too late and to bring people or groups of persons into agreement. Process mining techniques are beneficial because they help in the discovery of anomalous data.

Keywords: Fraudster, Fraud Detection, Types of frauds, Process Mining, Loan process

Dept. of Computer Science
Manipal University Jaipur
Jaipur, India
srivastavaswati2011@gmail.com
roheet.bhatnagar@jaipur.manipal.edu
Received: , Accepte

I. INTRODUCTION

Banking is a tool that allows banks to bridge the gap between funding sources and execution. "The acceptance, for the purpose of lending or investment, of money deposits from the public, repayable on demand or otherwise, and withdrawal by cheque, draught, or other means" is what banking means (Banking Regulation Act, 1949). The concept of banking, as we know it today, began in the late 18th century. Moneylenders were the ones who came up with the idea of taking deposits and issuing receipts, according to the Central Banking Committee of 1931.

It is unavoidable that such a large industry be subject to numerous frauds. "Despite having a powerful regulator, the financial services industry has emerged as the most vulnerable sector to

fraud,” according to a KPMG India fraud survey conducted in 2012[3]. Misuse of technology in the banking sector involves overpayments to suppliers or a self-bank account, exchanging potentially sensitive information, and using the company's technology tools for inappropriate activities such as overlapping business relationships. Additionally, delivering services on mobile and social media sites with a restricted understanding of security standards presents a significant risk to both consumers and financial institutions.” Employees topped the list as the single-largest perpetrators of fraud, accounting for 36 percent of the number, according to survey respondents. The banking industry has emerged as one of the most important markets, influencing the lives of ordinary people and corporations directly or indirectly. It is important to ensure that banking processes are both safe and stable. A banking security breach could result in significant losses. The loan mechanism is one of the most critical aspects of any banking system. It is a service offered by almost all banks that allows customers to take out a certain amount of credit based on their eligibility as determined by the bank and repay it over time with a certain interest capitalization. The credit (loan) can be used for a variety of reasons, including the purchase of new cars, the purchase of a home, educational purposes, business loans, personal loans, and so on.

II. WHAT IS A FRAUD

What is the concept of a fraud?

“An act or instance of deceit, an artifice by which the right or interest of another is hurt, a deceptive trick or stratagem,” according to the Oxford dictionary.

“Any of the criminal activities marked by deception, concealment, or breach of trust,” according to the IIA [7] International Standards for Professional Practice. These actions do not include the threat of violence or the use of physical power. Parties & organisations commit fraud to property, or services; acquire money, to gain a personal or business advantage or to prevent payment or loss of services.”

III. FEATURES TANGLED IN THE FRAUD:

Why do people defraud others? Donald Cressey, a well-known criminologist, suggested a fraud triangle model[8] to describe the factors that lead to anyone committing occupational fraud. It consists primarily of three components, which are described and explained below, and which lead to fraudulent behaviour:

1. Financial need/motivation that is perceived to be unshareable:

Another part of the fraud triangle is motivation, which is also known as incentive. It is the pressure or "need" felt by the individual who commits the fraud. It could be a genuine financial or other need, such as significant medical bills or debts. It may also be a perceived financial need, such as an individual who desires material goods but lacks the financial resources to obtain them.

2. Perceived possibility:

The willingness to commit a fraud can be described as opportunity. Since fraudsters do not want to be discovered, they must assume that their actions will not be detected.

3. Rationalization:

Employees may justify their actions by deciding that fraud is acceptable for a variety of reasons. In most forms of frauds, rationalisation is a critical part



Fig 1: The Donald Cressey hypothesis led to the development of the fraud triangle.

IV. PRINCIPAL MECHANISMS FOR FRAUD DETECTIONS:

Before we can understand the problems, we must first understand how fraud is currently identified in banks. The following are some of the methods for detecting a fraud:

1. Anonymous complaints/whistle blowers ("Public Interest Disclosure and Protection of Informer" (PIDPI)).
2. Internal audits or statutory audits at a central level
3. Vigilance Department Verification by Chance/Random

According to Deloitte's India banking fraud survey from 2012, 53 percent of respondents said fraud was discovered through internal audit reviews. The vast majority of cases were discovered as a

result of a formal or informal complaint process. Frauds were found by anonymous complaints and whistle blower mechanisms, respectively, according to 43 percent and 37 percent of respondents. However, the surprising result is that more than 20% of frauds were found by chance during vigilance department random checks. [9]

V. COMPLICATIONS IN FRAUD DETECTION:

1. The current systems, as mentioned above, have a flaw that makes them vulnerable to fraud detection. Within six months, the bulk of the frauds were found, with 23% discovered after a year [11]. As we all know, the longer the duration, the more significant the effects. Insider fraudsters typically take a "slow and steady" approach to committing fraud. To put it another way, the insiders stole "small" sums of money and carried out their crimes "slowly" over a long period of time, likely to escape detection. The lower half of the cases (those lasting less than 32 months) had an estimated actual monetary impact of \$382,750, while the upper half (those lasting 32 months or more) had an average actual monetary impact of \$479,000. [12]
2. Internal audits and Vigilance verifications are carried out on a sporadic basis. It is difficult to manually check each and every record because each branch would have thousands of records and most banks have undergone computerization and CBS. However, fraud does not occur at random. The fraudster devises his scheme in such a way that it is undetectable by a random search.
3. A lack of experience is also a major factor in fraud going undetected. Since the majority of our bank officials and internal auditors have no idea how a CBS works. How will the audit trail be verified? How to spot a thief in the act. This leaves a lot of space for a con artist to get away.
4. The vigilance departments of several banks are attempting to use technology to detect fraud. However, the conventional rule-based, descriptive questions, and analytics receive the majority of the attention. The majority of businesses employ spreadsheet and database software such as Microsoft Excel and MS Access. Although these tools are important in any data analytics programme, they are often used to match, group, order, enter, or filter data that is primarily descriptive. However, in general, these methods are sluggish and

ineffective at detecting fraud. Since these aren't designed for that. There are more advanced methods focused on process mining techniques that can be used.

VI. PROCESS MINING

The lost link between model-based process analysis & data-oriented analytical techniques is process mining. Data science expertise that can be specifically implemented in several domains to analyze and optimize processes. Data science is the career of the future and there will be no survival for companies that are unable to use (big) data smartly. Focusing on data storage & data processing is not enough. Data scientists also need to link data to process analysis. The difference between conventional model-based process analysis (such as simulation & other business process management techniques) and data-centric analysis techniques (such as machine learning & data mining) is bridged by process mining.

Process mining seek out confront event knowledge (i.e., observed behaviour) with process models (hand-made or discovered automatically). This technology has only recently become available but can be applied to any form of an operational process (organizations & systems). Examples of applications include evaluating hospital care procedures, improving international customer service processes, recognizing customers' browsing habits using a booking site, analysing luggage handling device failures, and improving an X-ray machine's user interface. Both applications have in common the need to link complex behaviour to process models. Hence, we refer to this as "data science in action".

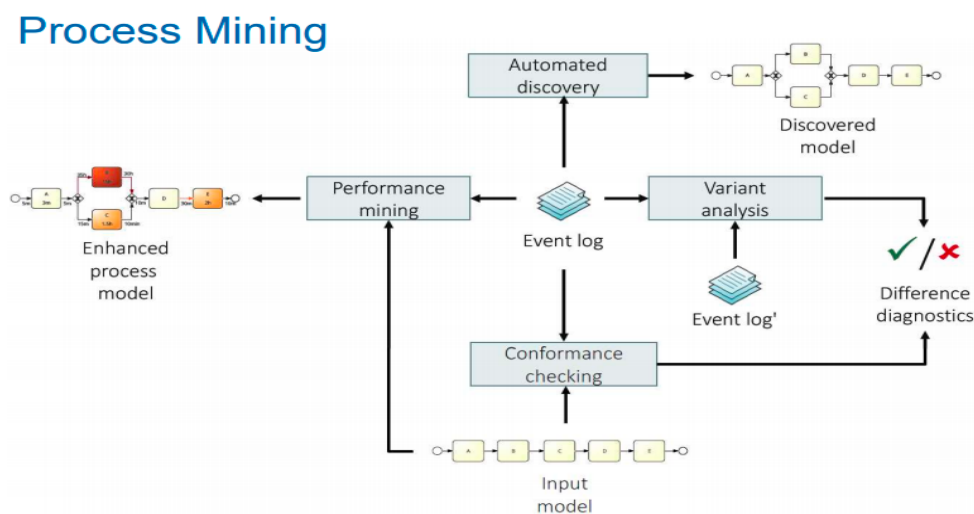


Fig. 2. Process Mining

VII. FRAUD DETECTION IN BANKS USING PROCESS MINING TECHNIQUES

Many different approaches have been used to detect fraud and malicious activities in various banking processes. The use of the process mining is quite efficient and reliable as this approach if implemented well, enact similar to that of humans' audit system with a difference that it can process a large amount of data in a more efficient and timely manner compared to that of humans. Some multiple algorithms and approaches have been used by researchers and scholars all over the world to accomplish this task. A few of them have been discussed with references as:

In Soane Lagraa et. al researchers have used process mining for behaviour change. A notion of behaviour change sequence has been introduced so that an irregularity can be identified if there is a pattern that has been identified as safe shows any unusual change. It uses a sequence event string that is used for processing the task. This sequence event string is a data set that denotes certain parameters that are eligible to be used in process mining. This method aims to identify a change in the attributes in the sequence events. The change here refers to an intrinsic change of attributes and parameters in the sequence event string. This change then finally helps to let the concerned authority know about malicious login events and behavioural changes in user login attempts. This can help decide whether the portal for the loan processing system has not been compromised.

In Dewi Rahmawati et al. researchers have used a heuristic miner algorithm in process mining for detecting fraud in the event logs of Good and Services Procurement. Heuristic Algorithms are efficient and provide more promising results of usage. Researchers have used the heuristic miner algorithm instead of the Alpha++ algorithm. The reason for using the heuristic algorithm is that it can calculate the frequency relation between activities in the logs to determine the causal dependency. It can also help in determining the dominance level of various processes consisting of thousands of logs as well as identifies the behaviours that are uncommon in any of the processes. Using the heuristic miner algorithm, researchers have got an accuracy of 88% with 120 test data and 13 error data. A threshold limit has been also used known as value fitness through which judgment of fraud and malicious activity can be inferred easily.

In Rafael Accorsi et al. researchers /reviewers surveyed the efficiency and potential of the process mining approach to accomplish the audit process of various business processes and business process management systems. Researchers have also put a major part of their efforts into the process discovery method. The process discovery method is the technique using which

a process event can be reconstructed as it was made by using a pre-defined approach. More particularly, the focus of the process discovery method is to reconstruct process structure from elements like event logs, data ow, etc. Based on this information gathered, researchers wanted to make adherence to the automation of security and privacy requirements of the business process.

In Michael Werner, researchers have worked on the visualization of the data obtained through process mining. The data source is considered to be financial audits. They have used an exceptionally good concept of materiality maps for data visualization. They have followed up an approach for process mining that helps in extracting the relevant and usable data. Further proceedings can be made accordingly and visualization of the data using a materiality map is made. This visualization methodology might helpful in detecting various patterns and also helps to judge certain faults that could detect fraud or malicious elements in the process.

VIII. IDENTIFICATION OF BANKING FRAUDS

A. Categories various types of Frauds in Banking Sector :

In virtually all the world's economies, the banking sector is one of the most important sectors, stemming from its large influence on the magnitude and direction of economic growth and transformation. [1] But in today's age, banks face immense challenges to produce a fair financial audit. Fraud detection is one such problem. Fraud is characterized as a concerted action by an individual or group of individuals to alter the truth or reality for selfish personal gains, and it has now become the single most real threat to the growth of the banking industry. [1] Fraud has led to the loss of vast sums of money in the financial sector and the economy of the nation in general. Fraud is an epidemic that has been eating deeply into the financial sector.

- 1. Internal fraud:** It is a fraud committed by employees and managers of an organization, operating either individually or in groups, or collusion with external parties. Management deception can be very difficult to identify because executives have access to most data and processes and can conceal their decisions because they realize that others do not necessarily question their choices. They will also pressure junior employees to commit fraud on their behalf. Ex: theft of credit, worthless deposits.

2. External fraud is fraud committed by businesses, such as manufacturers, rivals, associates, and consumers, involving third parties. Potential clients, governments & crime organizations comprise these criminals. The perpetrators may operate independently or may cooperate with the staff to defraud the bank.
3. Advance fraud: Banks offer advances to individuals, businesses, organizations for the benefit of their financial needs, such as house loans, transfers or loans for working capital facilities, conveyance or credit for services for working capital, company growth, etc.
4. Cyber fraud: With mechanisms such as phishing, keylogging, spyware, malware, and other internet-based fraud directly aimed at bank customers, the threat has pushed customers into cyberspace.
5. Deposit fraud: To gain money from depositors by posing as a bank or other financial entity fraudulently.
6. Off-balance sheet: typically means an asset or liability or operation of funding that is not on the balance sheet of the business. Complete return swaps are an example of an aspect of an off-balance sheet.

B. Statistics About Frauds in Banking

1. Numerous forms of identity fraud may be identified by customers. In 2018, more than one form of identity theft was included in 17% of identity theft statistics.

Source: Customer Sentinel Network, Federal Trade Commission.

Table 3: Data of frauds reported in the year 2018

<i>Type of identity theft</i>	<i>Number of reports in a year</i>	<i>Percent of total top 5</i>
<i>Credit card fraud — of existing accounts</i>	32,328	10.1
<i>Miscellaneous identity theft</i>	87,764	27.2
<i>Credit card fraud of new accounts</i>	1,30,938	40.51

<i>Mobile telephone—new accounts</i>	33,465	10.4
<i>Fraud in Tax</i>	38,964	12.1
Total	3,23,458	100.00%

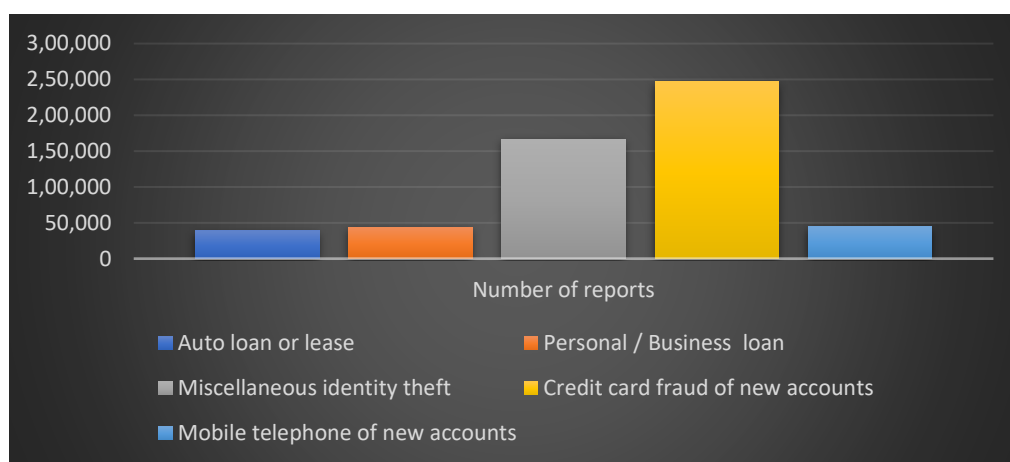


Fig 3: Statistical Representation of Identity Theft in the year 2018

- Numerous forms of identity fraud may be identified by customers. In 2019, more than one form of identity theft was included in 18% of identity theft statistics.

Source: Customer Sentinel Network, Federal Trade Commission.

Table 4: Data of frauds reported in the year 2019

<i>Type of identity theft</i>	<i>Number of reports</i>	<i>Percent of total top5</i>
<i>Auto loan or lease</i>	38,563	7.2
<i>Personal / Business loan</i>	43,914	7.9
<i>Miscellaneous identity theft</i>	1,66,873	30.8

<i>Credit card fraud of new accounts</i>	2,46,763	45.72
<i>Mobile telephone of new accounts</i>	44,210	8.3
Total	5,40,326	100.00%

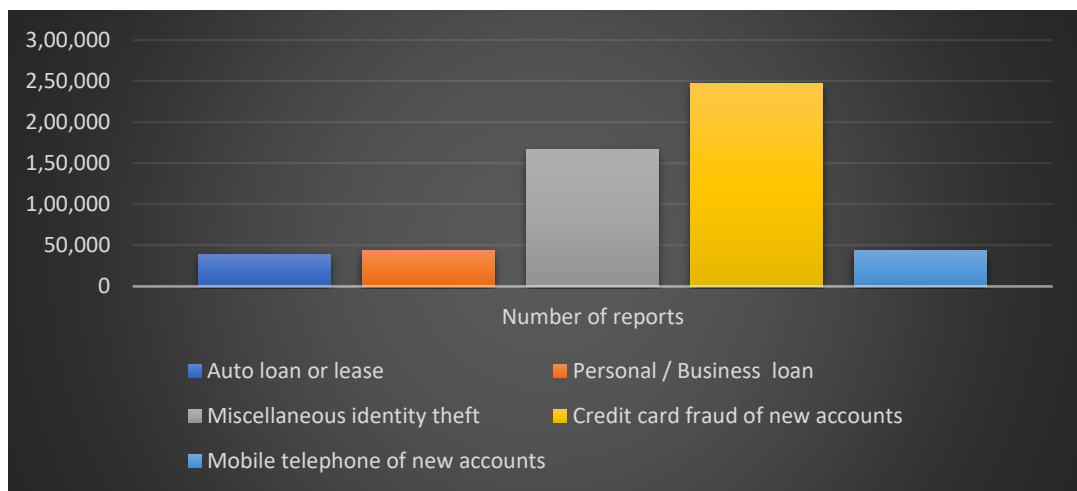


Fig 4: Statistical Representation of Identity Theft in the year 2019

- Percentages based on the total number of reports by calendar years from the Customer Sentinel Network. These figures exclude registry concerns about "Do Not Call". *Source: Customer Sentinel Network, Federal Trade Commission.*

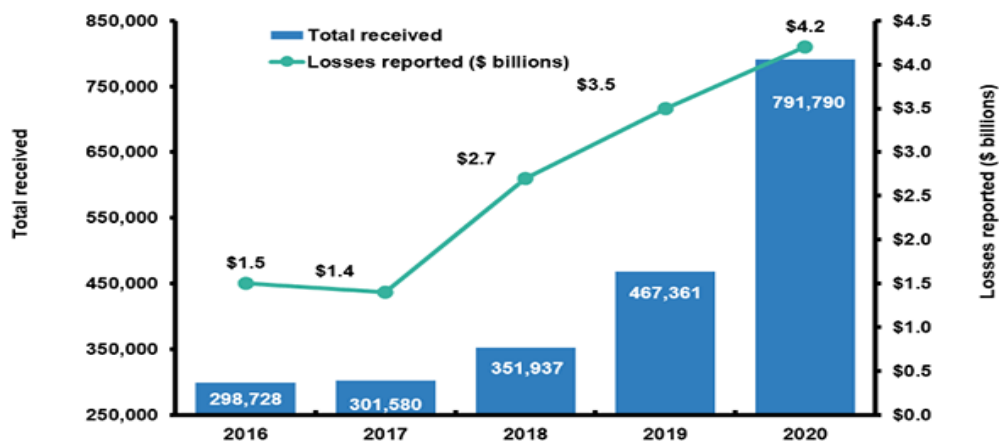


Fig 5: Identity Theft And Fraud Reports, 2015-2019

C. Classification of fraud

Table 3. Fraud by Insiders

Serial No.	Types	Description
1	Uninsured deposits	Asking a fake bank for deposits..
2	Wire Fraud	Fraudulent claims to acquire cash through cable, radio or television, etc.
3	Theft of identity	Fictitious bank workers use customers' personal details and abuse it.
4	Rogue Traders	Employees, on behalf of their boss, make illegal deals.
5	Demand Draft fraud	Fraud by insincere bank employees triggered by the misleading Demand Draft.
6	Fraudulent Loans	Loan lent by a fraudulent or non-existent individual under the control of a dishonest bank officer.
7	Forged documents	Documents used to hide trivial information through deception.

Table 4: Fraud by others

Serial No.	Types	Description
-------------------	--------------	--------------------

1	Counterfeit Credit Cards	Fraud by copying or skimming the data on the magnetic stripe of the card by creating copies of valid credit cards.
2	Bill Discounting fraud	Fraudulently discounting a large bank bill after gaining confidence with the bank.
3	Accounting Fraud	Creative accounting & cheat concealing of original financial status when dealing with bank.
4	Fake Currency Notes	Forgery of notes on currencies.
5	Forgery & altered cheques	Changing cheque entries & misusing them.
6	Stolen cheques	Stealing a hefty amount of cheque & misusing it.
7	Cheque Kiting	Usage of the float to make use of non-existent bank account assets.
8	Credit Card fraud	Fraud committed by use of payment card in a transaction.
9	Stolen Payment Cards	Misuse of credit or debit cards after some have stolen them.
10	Money Laundering	Any scheme whereby the true origin of funds is obscured.
11	Theft of identity & impersonation	By collecting customer details & using it to withdraw cash from the bank.
12	Internet fraud & phishing	Fraud via the internet by imitating it.

13	Fraudulent Loan applications	To cover a credit history riddled with financial difficulties by using fake information and receiving risky loans as a sound investment for a bank.
14	Skimming of card information	Fraud by connecting the card stripe reader to ATMs etc. in order to obtain unauthorized access to the magnetic stripe material.
15	Cyber Fraud	Tech fraud, such as computer fraud, etc.

D. Need of Process Mining in Banking

For banks covering every aspect of banking operations, these 5 reasons process mining is relevant and can make the difference between adopting the imperative of change and staying bound to outdated technology. The secret to better results in productivity and effectiveness is process mining in each case.

1. Enhancing internal and external compliance

For banks, process mining is vital as it can provide a seamless view of any external transaction or internal process from start to nish, allowing management to monitor the way the process unfolds. It can be automatically generated at any point where a compliance response is required. This helps ensure that banks act following the regulations under which they operate, by accelerating things such as reporting to authorities' suspicious transactions and reducing the potential for errors.

2. Managing the complexity of organization and process

Process mining can uncover in-depth, actionable information about how complex processes operate, as well as how they communicate within an organization with other processes. The use of process mining enables banks to view multiple systems as a cohesive whole within their organization, and multiple processes within those systems.

This overarching vision means that banks have the data they need to identify opportunities to renew their processes and/or standardize them as needed.

3. Innovation funding

Process mining helps banks and financial companies eliminate the risk of innovation by providing insights into the operation of internal systems and highlighting optimization opportunities. This enables banks to regard "innovation" as an ongoing transformation of the way they function, not as a small and disruptive occurrence.

4. Management of transition effectively

Process mining will soften the impact when change eventually happens by helping organizations make smarter, more open, and data-driven decisions. It removes the assumption that choices are being made for the wrong reasons, or that change is being introduced only for the sake of it. Process mining may be used as a monitoring device for the modifications themselves after any given period of transition, examining the health and efficacy of any new or modified systems, and fixing any negative aspects.

5. Exceeding wishes of clients

Process mining helps banks understand the behaviour of customers and connect their processes to forecast experiences through potential customer journeys. It is the interaction within an enterprise between the underlying processes and how, where, where, and why customers engage with those processes. Taking a customer-centred view of business processes ensures that banks can take advantage of customer viewpoints (consumers, employees, or other companies) and alter the way they work to deliver more meaningful customer experiences.

IX. FUTURE WORK: A BIGGER PERSPECTIVE

For banks covering every aspect of banking operations, these 5 reasons process mining is relevant and can make the difference between adopting the imperative of change and staying bound to outdated technology. The secret to better results in productivity and effectiveness is process mining in each case.

a. Enhancing internal and external compliance

For banks, process mining is vital as it can provide a seamless view of any external

transaction or internal process from start to finish, allowing management to monitor the way the process unfolds. It can be automatically generated at any point where a compliance response is required. This helps ensure that banks act following the regulations under which they operate, by accelerating things such as reporting to authorities' suspicious transactions and reducing the potential for errors.

b. Managing the complexity of organization and process :

Process mining can uncover in-depth, actionable information about how complex processes operate, as well as how they communicate within an organization with other processes. The use of process mining enables banks to view multiple systems as a cohesive whole within their organization, and multiple processes within those systems.

This overarching vision means that banks have the data they need to identify opportunities to renew their processes and/or standardize them as needed.

c. Innovation funding

Process mining helps banks and financial companies eliminate the risk of innovation by providing insights into the operation of internal systems and highlighting optimization opportunities.

d. Management of transition effectively

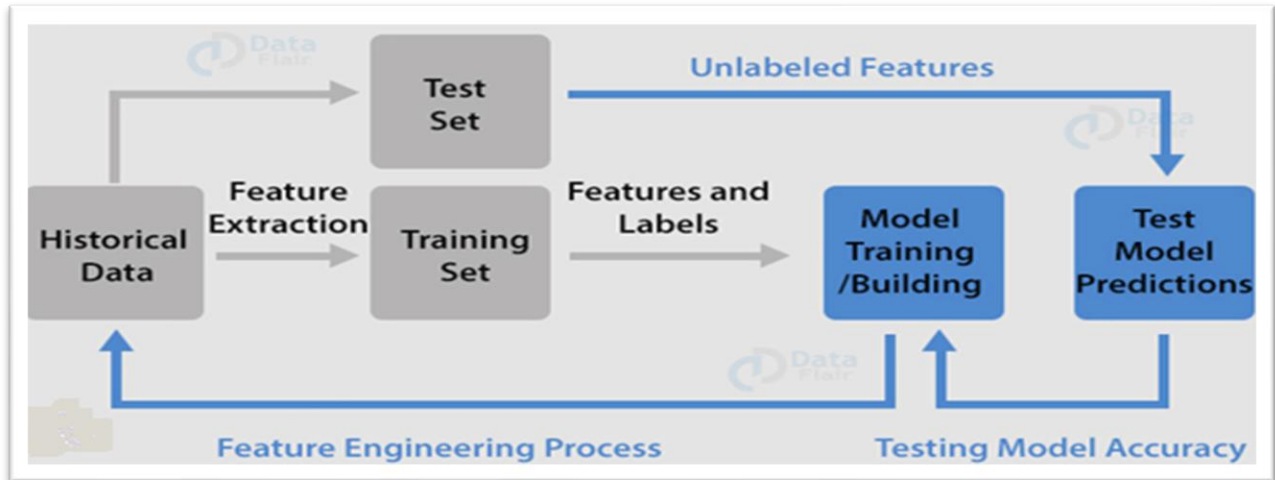
Process mining will soften the impact when change eventually happens by helping organizations make smarter, more open, and data-driven decisions. It removes the assumption that choices are being made for the wrong reasons, or that change is being introduced only for the sake of it. Process mining may be used as a monitoring device for the modifications themselves after any given period of transition, examining the health and efficacy of any new or modified systems, and fixing any negative aspects.

e. Exceeding wishes of clients

Process mining helps banks understand the behaviour of customers and connect their processes to forecast experiences through potential customer journeys. It is the interaction within an enterprise between the underlying processes and how, where, when, and why customers engage with those processes. Taking a customer-centred view of business processes ensures that banks can take advantage of customer viewpoints (consumers, employees, or other

companies) and alter the way they work to deliver more meaningful customer experiences.

Fig 6: Research Model for researching on Frauds on banking



IX. CONCLUSION

This paper explains what a banking scam is and how to avoid it. It then goes on to classify various types of frauds, their meanings, the factors that influence them, and the difficulties that come with detecting them. The paper lists and describes various process mining techniques and their general applications, as well as the best available process mining techniques for detecting insider fraud, as suggested by several researchers and currently used in various industries. We also shed light on the big data view of banking and fraud detection as part of our future work. In conclusion, we can say that fraud detection & prevention is a top priority for the banking industry, and process mining techniques can help reduce fraud cases significantly. To achieve the goal, we can use any or all of the methods mentioned above.

REFERENCES:

Baader, G. and Kremer, H., 2018. Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems*, 31, pp.1-16.

Badejo, B.A., Okuneye, B.A. and Taiwo, M.R., 2018. Fraud detection in the banking system in Nigeria: Challenges and prospects. *Shirkah: Journal of Economics and Business*, 2(3).

Becker, T. and Intoyoad, W., 2017. Context aware process mining in logistics. *Procedia Cirp*, 63, pp.557-562.

Bernardi, S., Alastuey, R.P. and Trillo-Lado, R., 2017, April. Using process mining and model-driven engineering to enhance security of web information systems. In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 160-166). IEEE.

Chiu, T., Wang, Y. and Vasarhelyi, M.A., 2020. The Automation of Financial Statement Fraud Detection: A Framework Using Process Mining. *Journal of Forensic and Investigative Accounting*, 12(1).

Chomyat, W. and Premchaiswadi, W., 2016, November. Process mining on medical treatment history using conformance checking. In 2016 14th International Conference on ICT and Knowledge Engineering (ICT&KE) (pp. 77-83). IEEE.

Du, J., Cai, H., Jiang, L. and Huang, C., 2017, November. Methods of Introducing Continuous Process Mining to Service Management for Mobile APPs. In 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE) (pp. 134-141). IEEE.

Eweoya, I.O., Adebisi, A.A., Azeta, A.A. and Amosu, O., 2019, August. Fraud prediction in loan default using support vector machine. In *Journal of Physics: Conference Series* (Vol. 1299, No. 1, p. 012039). IOP Publishing.

Flores, Isabel González, and Josué Rivera Riquenes 2020 "Audit 2.0, A Perspective For Its Execution In The Business Environment Using Process Mining Techniques." *Vivat Academia* 23.150: 47-57.

Ganesh, K., Dhanush, S. and SM, S.R., 2017, March. An approach to fuzzy process mining to reduce patient waiting time in a hospital. In 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-6). IEEE.

Gupta, M., Sureka, A. and Padmanabhuni, S., 2014, May. Process mining multiple repositories for software defect resolution from control and organizational perspective. In *Proceedings of the 11th Working Conference on Mining Software Repositories* (pp. 122-131).

Hashim, H.A., Salleh, Z., Shuhaimi, I. and Ismail, N.A.N., 2020. The risk of financial fraud: a management perspective. *Journal of Financial Crime*.

Hevia, D., 2017. *Audit and Accounting Guide Health Care Entities*.

- John, S.N., Anele, C., Kennedy, O.O., Olajide, F. and Kennedy, C.G., 2016**, December. Realtime fraud detection in the banking sector using data mining techniques/algorithm. In 2016 international conference on computational science and computational intelligence (CSCI) (pp. 1186-1191). IEEE.
- Lagraa, S., & State, R. 2020**, April. Process mining-based approach for investigating malicious login events. In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium (pp. 1-5). IEEE.
- Moreira, C., Haven, E., Sozzo, S. and Wichert, A., 2018**. Process mining with real world financial loan applications: Improving inference on incomplete event logs. *PLoS One*, 13(12), p.e0207806.
- Mwangi, S.W. and Ndegwa, J., 2020**. The Influence of Fraud Risk Management on Fraud Occurrence in Kenyan listed Companies. *International Journal of Finance & Banking Studies* (2147-4486), 9(4), pp.147-160.
- Putri, E.S.G. and Tobing, R.P., 2019**, October. Auditor Switching and Initial Audit Procedures: A Case Study. In 3rd Asia-Pacific Research in Social Sciences and Humanities Universitas Indonesia Conference (APRISH 2018) (pp. 205-211). Atlantis Press.
- Rahmawati, D., Sarno, R., Fatichah, C. and Sunaryono, D., 2017**, October. Fraud detection on event log of bank financial credit business process using Hidden Markov Model algorithm. In 2017 3rd International Conference on Science in Information Technology (ICSITech) (pp. 35-40). IEEE.
- Rahmawati, D., Yaqin, M.A. and Sarno, R., 2016**,
- Rambola, R., Varshney, P. and Vishwakarma, P., 2018**, December. Data mining techniques for fraud detection in banking sector. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-5). IEEE.
- Srivastava, S.,et.al 2021**. Process Mining Techniques for Detecting Fraud in Banks: A Study. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(12), pp.3358-3375.
- Srivastava, S. and Bhatnagar, R., 2019**, A study about Process Mining. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.
- Srivastava, S., Srivastava, G. and Bhatnagar, R., 2019**, Analysis of Process Mining in Audit Trails of Organization. In International Conference on Information Management & Machine Intelligence (pp. 611-618). Springer, Singapore.

Srivastava, S., Srivastava, G. and Bhatnagar, R., 2021. Green Cloud. In *Smart Agricultural Services Using Deep Learning, Big Data, and IoT* (pp. 69-80). IGI Global.

Hansrajani, K., Johnson, M.B. and Srivastava, S., 2019. Cyber Security. *Journal of Advancements in Robotics*, 6(3), pp.25-28.

Srivastava, S. and Srivastava, G., Tools and Techniques for Network Forensics.

Van Eck, M.L., Sidorova, N. and van der Aalst, W.M., 2017, July. Guided interaction exploration in artifact-centric process models. In 2017 IEEE 19th Conference on Business Informatics (CBI) (Vol. 1, pp. 109-118). IEEE.

Werner, M., 2019, January. Materiality maps—process mining data visualization for financial audits. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

Yazici, I.E. and Engin, O., 2019, July. Use of Process Mining in Bank Real Estate Transactions and Visualization with Fuzzy Models. In International Conference on Intelligent and Fuzzy Systems (pp. 265-272). Springer, Cham.

Zanatta, A.L., Steinmacher, I., Machado, L.S., de Souza, C.R. and Prikladnicki, R., 2017. Barriers faced by newcomers to software-crowdsourcing projects. *IEEE Software*, 34(2), pp.37-43.