APPLICATION OF AI IN FRAUD DETECTION IN BANKING INDUSTRY

Bhavya Menon,PGDM
Universal Business School
Karjat, India
bhavya.menon@ubs.org.in

Kehaan Nooshian, PGDM+GMP (Cardiff Metropolitan University)
Universal Business School
Karjat, India
kehaan.nooshian@ubs.org.in

Akanksha Sahu, PGDM + GMP (Cardiff Metropolitan University, U.K),
Karjat, India
akanksha.sahu@ubs.org.in

I. ABSTRACT

The banking system is crucial to capital formation and trade facilitation in the modern economy. The level of stability in a nation's banking and financial system influences how much it produces and consumes in terms of goods and services. It serves as a clear barometer of its population's welfare and standard of living. India's banking ecosystem has been growing relentlessly and the adoption of AI is constantly evolving, which has the potential of enabling a digital banking infrastructure. A 2022 survey by PWC in collaboration with FICCI revealed that India's banking sector is leading in implementing and adopting all emerging AI use cases. Artificial Intelligence (AI) has significant potential to improve the detection of financial fraud quicker, more effectively, and by removing rising amounts of false signals far more efficiently. Machine learning models, pattern recognition, anomaly detection, behavioral biometrics, network analysis, image, and video analysis, etc. have become means of extreme value when detecting fraud.

Despite significant developments in the Indian banking industry and integration of AI in its system, it currently lacks the right tools and technologies in place to detect signals of fraud, along with weak regulatory policies and skilled workforce. Although the cumulative losses attributable to fraud for PSBs and private sector banks have decreased to 28,000 crores from 65,900 crores in FY'21, and from 39,900 crores to 13,000 crores in FY'22, thanks to the RBI's intervention through its regulatory frameworks such the Early Warning System framework, the number of fraud charges has increased from 5,916 to 9,103 instances over the past five years.

Through an analysis and data from various sources, the paper tries to examine various kinds of frauds committed in the banking industry and the current challenges in the existing approaches for fraud detection in India. It highlights the role of Artificial Intelligence in fraud detection and the degree its implementation in Indian banks vis-a-vis foreign banks. Overall, this research paper constructively contributes towards providing a comprehensive understanding of the ongoing trends in the Banking system for fraud detection and the scope for improvement.

II. INTRODUCTION

a) Classification of Frauds:

According to the provision of the Indian Penal Code, 1986, RBI has issued a Master Directive in2016 with the following guidelines to report as 'Fraud' for maintaining uniformity in reporting:

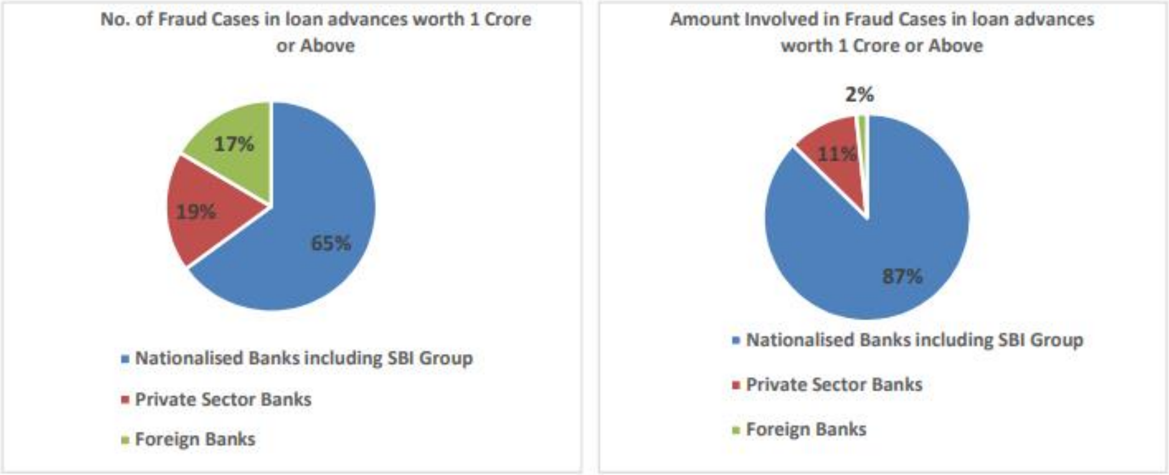
- Misappropriation and criminal breach of trust.
- Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property.
- Unauthorized credit facilities are extended for reward or for illegal gratification.
- Cash shortages.
- Cheating and forgery.
- Fraudulent transactions involving foreign exchange
- Any other type of fraud not coming under the specific heads as above.

b) Types of Frauds:

There are several forms of fraudulent transactions in the financial industry. The following are broad categories of financial fraud happened:

- **Deposit-Related frauds**

When money is deposited into a bank account via an electronic or paper payment, deposit fraud happens. The person opens the bank account and gives the fraudster(mules) access to the deposit. Banks in the UK found 8,500 money mule accounts in 2017. Banks have blocked the usage of deposits used for fraud and money laundering since 2018 by freezing £60 million in 88,000 bank accounts. Almost 95% of deposit-related scams in the last four years have occurred in commercial banks, accounting for around 67% of the total amount engaged in fraud in India. The number of frauds has dropped recently as a result of a new payment system, commercial banks' deployment of the check truncation system (CTS), the use of electronic fund transfers, etc. Public sector banks, which are notorious for large-scale frauds, stand in stark contrast to private sector banks, which account for only around 18% of fraud cases but 83% of the overall amount involved. The occurrence of high-value bank loans as a result of collusion between corporate entities and senior bank officials is a sign of subpar corporate governance. Online, cyber, and technology-related frauds are blamed for the private banks' large number of fraud cases and comparatively low cost of fraud.



Note: Data pertains to the period from March 31, 2010 to March 31, 2013.
Source: Chakrabarty (2013).

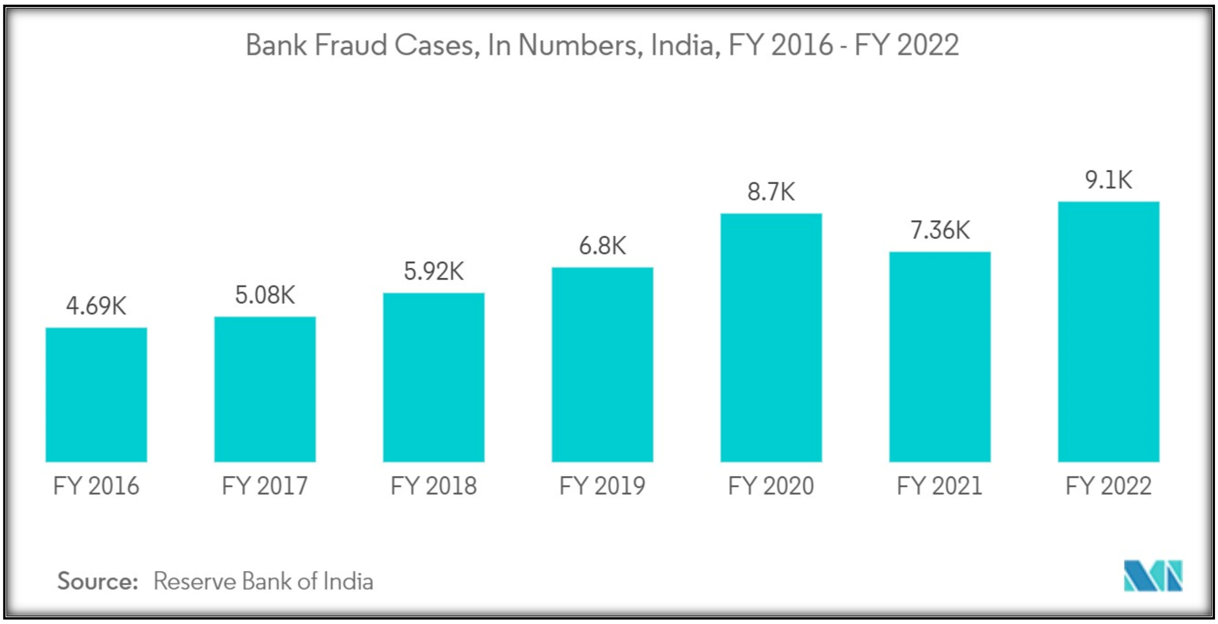
Chart 1. Proportion of Banks in number of fraud incidents and amount involved in Deposit-frauds

- **Higher-Advance-related Frauds**

In comparison to private sector banks, higher advance-related frauds involving loans totaling more than Rs. 1 crore tend to occur in public sector banks. This is a result of lending for significant and protracted projects in the infrastructure, energy, and mining industries. The NPAs rise as these projects advance, which is frequently linked to more lending to and exposure to projects in the mining, infrastructure, and power sectors. These projects' performance and related cash flows closely track the boom-and-bust economic cycle. One drawback is that during an inspection, bankers tend to take projects at face value, so the original costing base of asset assessment does not indicate any financial loss. The project fails and these cash flows are unrealizable a result of a lack of diligence in checking the approvals.

- **Third-party Frauds**

Big-scale loan advance frauds are difficult to pull off, and they frequently originate from bank employees conspiring with borrowers and occasionally even with representatives of unrelated parties like lawyers or chartered accountants (CAs). According to studies, India lacks qualified auditors. Low standards have been imposed and early warning signals (EWS) have not been detected, which has led to an increase in malpractice. Also, the incentive system for employees has to be reviewed because they receive no compensation for reporting fraud or blowing the whistle on it. Frauds also happen as a result of staff members not being aware of proper procedures in place and warning signs they should be aware of. The main cause of technology-related fraud is employees' non-compliance with established standard practices and processes.



Source: Reserve Bank of India

Chart 2. Bank Fraud cases from FY 2016-2022

III. CHALLENGES IN THE INDIAN BANKING SYSTEM TO IMPLEMENT AI

The astounding interconnection of all the bank servers connected with AI has resulted in the financial system being more seamless. Despite this, the Indian banking industry's use of AI is still in its infancy due to a lack of infrastructure, a rise in technological complexity, and labour attrition. As a result of cyber threats, the banking industry is frequently targeted by phishing, sim-swap scan, credit card fraud, Keylogging, email spoofing, vishing, spamming, and Watering hole scams.

IV. OBJECTIVES

1. To understand different types of technical banking frauds committed, especially in India
2. To perform a comparative study of National banks and foreign banks in terms of the implementation of AI in fraud detection.

V. LITERATURE REVIEW

AI has been playing a significant role in detecting fraud in addition to improving credit scores, improving customer service, and reducing dangers from scams. Owing to the daily increase in electronic transactions and the e-commerce industry, cyber systems have come under intense attack, making cyber security essential for all banks and other financial institutions. Almost 4.8 thousand instances of internet banking fraud were recorded in India in 2021. There were significantly more instances of banking fraud this year than in the previous one. Major banks in the US utilize Shape Security software to identify phony users and prevent gift card fraud, credential stuffing, and fraudulent credit application activity. (Kochhar, Purohit, & Chutani , 2019) **(Kochhar, Purohit , & Chutani , 2019)**

For banks, AI has greatly improved credit management. The lengthy procedure that goes into processing advances and verifying information goes through several stages. Large data sets can be accessed simultaneously in real-time with the use of powerful AA/ML models, assisting banks in evaluating new clients, pricing their instalments based on the loan amount, and paperwork, and lowering the risk of fraud**. (Alhaddad, 2018)**

While the improved capacity of commuting technology undoubtedly provides benefits, there are also drawbacks. Since new forms of cybercrime are developed every day, it is challenging to identify and address these issues. Yet, new security automation has made it easier to spot the behavioral pattern of activity for all user accounts or devices. Fraud was prevented because the malicious agent's single point of attack allowed for accurate response time identification. **(Soni, 2019)**

Since banks house client data, they have been the main targets for hackers. As a result of this and the rising trend of credit card use, there were billion-dollar losses due to credit card fraud in 2017. When a credit card is stolen, it resembles identity theft in which an unauthorized transaction is performed by the intruder possessing the card. Due to the magnitude of financial transactions involved, credit card fraud that results from a stolen, lost, or counterfeit card is challenging for the banking industry. The skewness of credit card fraud data sets, which arises from the fact that the number of fraudulent transactions is far lower than the number of legitimate transactions, makes it difficult for AI and ML to effectively detect such fraud. Credit card fraud detection systems must be incredibly responsive in the real world as well. The digital architecture must be swift enough to hold the enormous volume of data generated every day. **(Btoush, Zhou, Gururaian, Chan, & Tao, 2021)**

While it was highlighted in another work that while AL algorithms may perform well in research settings, they often miss the mark when it comes to important commercial issues. It has also been established that the general public, in addition to businesses and institutions, is impacted by payment fraud. Payment card fraud is a method used by criminal organizations and Organized Crime Groups (OCGs) to finance their operations, which include the use of weapons, drugs, and terrorism endangering people's life.
Instant Payments (IP) are anticipated to make fraud detection more difficult, and the European Central Bank and the Central Bank of the Russian Federation have already suggested implementing IP systems. In contrast to traditional Single Europe Payment Area (SEPA) transactions, fraud detection for immediate payments must be finished in a matter of seconds rather than a day or more. The two types of online fraud that have been occurring most frequently are "clean fraud" -where fraudsters get legitimate cardholder information, such as 3D Secure and Address Verification credentials and "friendly fraud," in which the beneficiary first completes a legitimate transaction before claiming that their card was used fraudulently and demanding a refund. **(Kurt, Alexander, & Alexand, 2019)**

"Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models," addresses the issue of false positives in bank payments, critiquing the present fraud detection method and its inefficiency. They aim to improve the efficiency of bank fraud detection measures by implementing a 'rules induction technique' framework in which new rules are generated by implementing tree-based ML algorithms such as Decision Tree and Random Forest, which are aimed at identifying cases that are currently incorrectly classified as fraud. Over the first part of the year, the framework was tested in a genuine fraud-monitoring system of a significant bank. The rules developed utilizing this framework proven to be sufficiently efficient while also having a clear commercial impact.
(Vorobyev & Krivitskaya, 2022)

Many aspects of internet banking frauds, how they provide a significant challenge to existing fraud detection approaches and data mining models, and how they display low efficiency and/or accuracy when directly applied to online banking fraud detection using numerous examples. They also offer an efficient online banking fraud detection framework that creates appropriate resources and consolidates several advanced data mining techniques, and they conclude that experimentations to test the efficacy of the said system proved to be not only successful, but also more accurate and with lower alert volume. **(Wei et al., 2012)**

The paper focuses on the rise in credit card frauds as it gains popularity for both online and regular transactions with the rapid advancement in the electronic commerce technology. As a consequence of the evolution of various credit card fraudulent transactions, it gives a study of many contemporary approaches based on Artificial Intelligence that are employed in credit card fraud detection mechanisms such as Data mining, Neural Network, Bayesian Network, Fuzzy logic, Artificial Immune System, K- closest neighbor algorithm, Support Vector Machine, Decision Tree, Fuzzy Logic Based System, Machine learning, Sequence Alignment, Genetic Programming, and so on. **(Tripathi & Mahesh, 2012)**

In their research paper entitled “Application of Artificial Intelligence and Its Powered Technologies in the Indian Banking and Financial Industry: An Overview” that although the Indian banking sector has been uncompromisingly incorporating AI-enabled technologies in their business operations in recent years, and while a large number of commercial and industrial banks worldwide have incorporated AI and its allied technologies for managing customer and back-office related activities, implementation of AI and its allied technologies is not at the level of advanced countries (BFSI, 2019). AI is the paramount of technology, capable of analyzing an individual's previous spending patterns and behavior towards numerous transactions and identifying irregularities. AI can also comprehend information based on experience; if it discovers an anomaly in regular transactions and corrects it, the AI helps the system to learn from that experience and make smart judgements on what can and cannot be considered fraud**. (Malali & Gopalakrishnan, 2020)**

Fraud has been a huge concern in the financial industry, and one of the critical areas in the banking sector where artificial intelligence systems have excelled the most is fraud detection. They characterize AI as very good at discovering trends in real time since it employs algorithms to examine patterns and predictive analytics to restrict fraudulent transactions, hence assisting banks in preventing financial fraud. They also use the FICO Falcon fraud assessment system as an example, which is based on a neural network shell, to demonstrate the deployment of sophisticated deep learning-based artificial intelligence systems today and conclude that fraud detection has made significant progress and is expected to continue in the coming years. **(Kaur et al., 2020)**

AI applications have are capable of making the banking sector robust and efficient; it specifically discusses various kinds of frauds in the banking industry such as phishing scams, Unauthorized transactions, Identity theft along with AI based strategies for detecting and preventing fraud such Integrating Supervised and Unsupervised AI Algorithms, Applied behavioral analytics, Creating Models from Massive Datasets, reviews the use of AI fraud detection and prevention vs traditional techniques. It concluded that AI based fraud detection and prevention systems are far more effective and efficient but sizable budget, specialized infrastructure, staff skill sets etc. are the only factors keeping banks from implementing the same. **(Alhaddad, 2018)**

The stages of artificial intelligence and several kinds of AI are described in the study. A number of BFSI areas have been discussed, including the current state of AI in each. With the banking industry in mind, it appears that the Central Bank of India has adopted a cautious but practical approach to utilizing modern technologies. Founded by Indian banks to promote retail payments, Bank Chain, which SBI first announced in 2017, is a 30+ member consortium made up of banks, NBFCs, and the National Payments Corporation of India (NPCI). It has been developing and putting Blockchain technologies into practice. Also, it has been mentioned that the accuracy of anti-money laundering and credit card fraud detection can be improved via anomaly detection. (Vijai, 2019)

VI. RESEARCH GAP

- The study on the use of AI in fraud detection in the banking industry is inadequate, particularly in the context of Indian Banking industry.
- There is less information regarding the usage of AI in fraud detection as compared to its integration in the front end.

VII. RESEARCH METHODOLOGY

The Secondary data used to understand the most common frauds occurring in the banking sector, the existing methods for detecting them, and how AI plays a significant part in this was acquired from various academic papers, journals, and research materials. Two databases were used to build arguments and understand the existing situation:

- **Scopus:** Scopus, is a database of peer-reviewed literature citations and abstracts from Elsevier. It is the largest abstract and citation database of scientific journals, books, and conference proceedings that have undergone peer review.
- **ResearchGate:** ResearchGate.net is a social networking and academic profile site that is a well-known online hub for exchanging academic articles. With over 135 million papers, it has a network of over 20+ million researchers.

Six banks from both domestic and foreign peers served as the focus group for this study. To understand the stage of AI deployment in their banking systems and growth potential, ICICI Bank, HDFC Bank, and Bank of Baroda were picked from India, while Citi Bank, DBH Bank and Danske Bank were chosen from American and Nordic countries. To help with the construction of this research article, it was feasible to identify the often occurring frauds, examine the typical tactics used for fraud detection, and identify the research gaps attributable to a Descriptive study design from the selected database. In-depth summary statistics over the last ten years from 2012-2022 and case study analysis were the methodologies employed to identify the obvious difficulties that AI has in spotting these frauds. Using a Qualitative Comparison analysis of Indian, American & Nordic banks, it was possible to observe the scope of AI and helped in making a few recommendations. The research gaps in the literature review also helped in recognizing the potential for further AI development in this field.

VIII. STRATEGIES USED FOR IMPLEMENTATION OF AI & ML IN THE SYSTEM

Banks have typically discovered that utilizing AI to detect fraud is significantly more effective and quicker. A thorough investigation to learn about the various fraud detection methods now in use helped to determine the following strategies: -

- **Developing a customer profile:** Banks need to be aware of typical consumer behavior to detect fraud accurately. Future behavior can be predicted by categorizing different consumer behaviors and creating profile clusters on them.
- **Fraud investigation:** With a thorough understanding of consumer behavior to prevent any imitation of purchasing behavior, AI creates patterns using ML. This then gives AI the ability to decide whether or not it matches a pattern or deviates far enough from the typical to be detected.
- **Persecuting false claims:** Neural networks take this capability a step further by making choices in real-time, whereas machine learning algorithms can analyse hundreds of thousands of transactions per second. These technologies enable the elimination of several flagged transactions.
- **Cyber-related fraud prevention:** Attacks by security apps or crimes like mail phishing or identity fraud are prevalent. In these situations, without requiring the user to read the email, ML algorithms can distinguish between real and spam email addresses based on the text, subject lines, and email data. Increased dataset input to the computer, continuous development of Classification models, and multi-factor authentication all play major roles in combating these frauds.

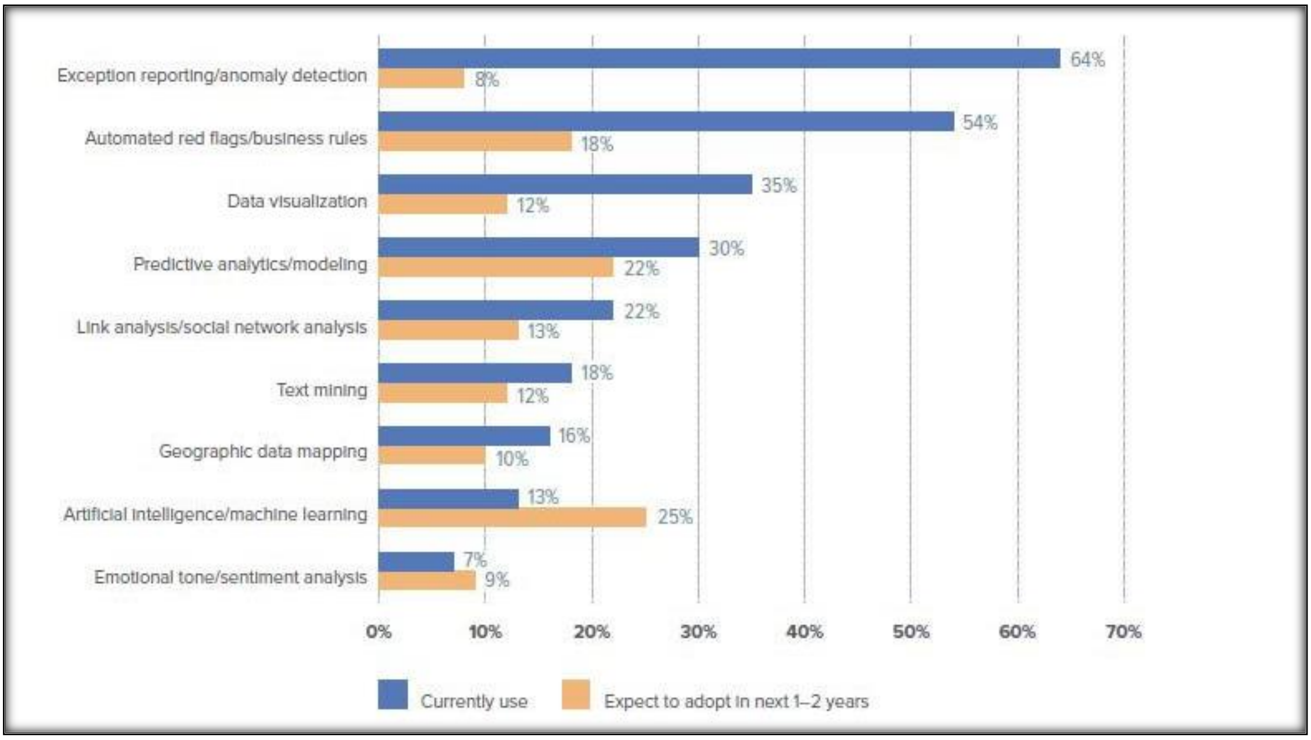


Chart 3. Fraud identification techniques used in AI by Banks

IX. COMPARATIVE STUDY BETWEEN THE SYSTEMS IMPLEMENTED IN INDIAN & FOREIGN BANKS FOR FRAUDS DETECTION

AI is being used by Indian banks to recognize human behavior, boost efficiency in automated operations, and cut costs for iterative tasks. A 2022 survey by PWC in collaboration with FICCI revealed that India’s banking sector is leading in implementing and adopting all emerging AI use cases.

In 2020, the total assets of public sector banks were $1.52 trillion. Additionally, bank credit increased at a CAGR of 3.57% between 2016 and 20. As the country's financial system expands, AI usage will continue to increase, allowing a digital banking infrastructure.

Markets forecasts the Fraud Detection and Prevention Market to grow from USD 19.5 billion in 2018 to USD 63.5 billion by 2023, at a CAGR of 26.7% during the forecast period. The major factors that are expected to be driving the FDP market are increasing revenue losses for organizations due to the rising fraudulent attacks, increasing use of electronic transactions across all the verticals and the sophistication level of cyber-attacks across the globe.

a) HDFC & DBS BANK

HDFC, have invested in 24x7 operational centers for constant monitoring and analysis of traffic in real-time with instant incident response. They also have teamed up with leading vendors in AI along with initiating a startup engagement program for fintech companies which would help detect frauds easily, including complex frauds that cannot be detected by traditional security and event monitoring tools. The challenges faced by HDFC are the capacity of hackers to launch the distributed denial of services (DDoS) type of attacks that makes the infrastructure unavailable for a longer period of time, concerns regarding API security and the need for the right people to develop the APIs, have the right processes.

The "transaction surveillance" function at DBS Bank, the largest bank in Singapore and Southeast Asia, has been using AI for many years to assess alerts generated by a rule-based system. The regulations evaluate transaction data from numerous systems throughout the bank, including those for consumer, asset, institutional, and payments banking. All of these transactions go through the rule-based system for screening, and the rules highlight transactions that fit criteria linked to someone or something engaging in potentially money-laundering transactions with the bank. The majority of the alerts produced by rule-based surveillance systems are false positives, accounting for up to 98 per cent of them. The deal in some way sets off a rule that causes the transaction to be flagged and placed on the alert list. However, a human analyst's follow-up inquiry reveals that the alerted transaction is not, in fact, suspicious

A few years ago, DBS started a project to apply the new generation of AI/ML capabilities in combination with the existing rule-based screening system. The combination would enable the bank to prioritize all the alerts generated by the rule-based system according to a numerically calculated probability score indicating the level of suspicion. The ML system was trained to recognize suspicious and fraudulent situations from recent and historical data and outcomes.

DBS also developed other new capabilities to support the investigation of alerted transactions, including a Network Link Analytics system for detecting suspicious relationships and transactions across multiple parties. Financial transactions can be represented as a network graph showing the people or accounts involved as nodes in the network and any interactions as links between the nodes.

After a thorough study of these two banks, it was observed that HDFC has teamed up with leading vendors in AI to detect frauds easily, including complex frauds that cannot be detected by traditional security and event monitoring tools, but they're still using primitive AI rule-based systems to detect frauds which can be outsmarted by organized crime groups. There's also a severe lack of skilled workforce to assist the said AI systems, while DBS that once used rule-based AI systems but after realizing its lack of accuracy and several cases of false positives, it started a project to apply the new generation of AI/ML capabilities in combination with the existing rule-based screening system. Which enabled the bank to prioritize all the alerts generated by the rule-based system according to a numerically calculated probability score indicating the level of suspicion. It already had a "transaction surveillance" function where the skilled workers monitored and supervised their old and New AI systems.

b) ICICI & CITIBANK

ICICI Bank is one of India's largest private sector banks, and it has implemented an AI-powered fraud detection system to identify and prevent fraudulent transactions in real time. The system uses machine learning algorithms to analyses customer behavior and detect anomalies that may indicate fraudulent activity. One of the benefits of ICICI Bank's AI system is its ability to identify potential fraud in real time, allowing the bank to take immediate action to prevent losses. Additionally, the use of AI has improved the accuracy of fraud detection, reducing the number of false positives and minimizing the need for manual intervention [1].

However, one of the challenges of ICICI Bank's AI system is that its effectiveness is highly dependent on the quality and quantity of data available and the risk of algorithmic bias. To ensure that the system is as accurate as possible, the bank must constantly collect and analyses large amounts of customer data. Additionally, the AI system may generate false positives, leading to unnecessary investigations and operational costs [2].

AI models can be biased if the data used to train them is biased, which can lead to incorrect predictions and decisions. Therefore, it is essential to ensure that the data used to train AI models is diverse and unbiased. Finally, AI models need to be continuously monitored and updated to ensure that they remain effective in detecting new types of fraud and adapting to changing fraud patterns [3]

Citibank is a foreign bank that has also implemented an AI-powered fraud detection system to improve the accuracy of fraud detection and reduce false positives. The bank uses advanced analytics and machine learning algorithms to identify patterns and anomalies in customer behavior that may indicate fraudulent activity. One of the benefits of Citibank's AI system is its ability to analyses large amounts of data, allowing the bank to identify subtle patterns that may be missed by humans. Additionally, the system can reduce false positives, saving time and resources for the bank [4].

Citibank faced several challenges in implementing AI in its fraud-detecting systems. One of the challenges was having a weak core technology and data backbone, another challenge was an outmoded operating model and talent strategy [5]

However, Citibank partnered with Feedzai, a fintech startup, to integrate their AI platform for risk management and fraud detection in banking [6]

Another challenge of Citibank's AI system is ensuring the privacy and security of customer data. The system relies heavily on customer data to identify potential fraud, which can be a concern for customers. Additionally, the bank must ensure that the AI system is secure and cannot be hacked by cybercriminals [7].

After comparing AI-powered fraud detection systems of both the banks we found that the system used by ICICI Bank depends greatly on the quality and amount of data available, and if the data used to train the system are biased, there is a risk of algorithmic bias. Citibank encountered difficulties integrating AI into its fraud-detection systems, but it overcame them by collaborating with a fintech company. Customers may be concerned about Citibank's responsibility to protect the confidentiality and privacy of their personal information.

c) BANK OF BARODA & DANSKE BANK

Bank of Baroda M S University in Vadodara has accepted Bank of Baroda's proposal to establish an AI center on its campus. In an endeavor to set the infrastructure for handling financial scams, it is being done.

They currently use AI for ATM predictive maintenance using external sensors and internal data points of failure, cash forecasting at currency chests, and other applications. **(Money Control, 2019)**

A leading provider of financial services in the Nordic region, Danske Bank, collaborated with Think Big Analytics, a Teradata company, to develop and introduce a cutting-edge platform for AI-driven fraud detection. With the help of a **deep learning algorithm**, it has updated its antiquated rules-based fraud detection system, which has a 60% decrease in false positives and a 50% boost in fraud detection capability. While some situations were forwarded to human analysts for additional examination, the new system also automated critical choices.

In order to deliver actionable knowledge regarding actual and fake fraudulent activity, the engine uses machine learning to assess tens of thousands of hidden variables and score millions of online banking transactions in real-time. Danske Bank enhances its overall efficiency and is now prepared for growth by drastically lowering the cost of reviewing false-positives. **(Donahue, 2017)**

X. INSIGHTS INTO WHY AI IS THE FUTURE OF ONLINE FRAUD DETECTION

The latest research projects provide light on why artificial intelligence (AI) is the future of online fraud detection. According to the inaugural Anti-Fraud Technology Benchmarking Report from the Association of Certified Fraud Examiners (ACFE), the amount firms are projected to spend on AI and machine learning to combat online fraud will treble by 2021. According to the ACFE report, just 13% of firms already employ AI and machine learning to identify and discourage fraud. According to the research, another 25% want to implement these technologies in the next year or two, representing a roughly 200% rise. According to the ACFE report, AI and machine learning technologies will most likely be used to combat fraud in the next two years, followed by predictive analytics and modelling.

XI. DATA ANALYSIS AND FINDINGS

- Implementing a fraud management solution would benefit from the **Rule-based** and risk analytics provided by the National Payments Corporation of India (NPCI). India's initial move towards consumer protection is the implementation of **multi-factor authentication** as part of a rule-based system, despite the fact that the Indian banking ecosystem lacks the infrastructure for Real-Time-Decline (RTD), to deny any suspicious and irregular transactions.

- While foreign banks like HSBC ML are implementing solutions to graphically group customer data based on financial behavior and make predictions based on connections between data, Indian banks are using outdated legacy and rule-based systems and predictive analytics that result in a high number of false positives.

- While most models rely on machine-led data based on digital transactions, Indian banks now rely primarily on customer-initiated data that is particularly prone to inaccuracies. Just **32% of India's 68% smartphone users have adopted e-banking** (mobile apps and online payments) as of 2020. This was also only made possible after 2016 when the ruling government pushed for banking infrastructure in rural India, demonetization, and the digitalization of the economy. Now 3.4 crore customers are active on digital channels; owing to the COVID-19 pandemic, the customer base almost tripled to 7.6 crores in 2020-2021. **(Rathore, 2022)**

- The privacy policies introduced by the RBI pose a challenge in regulating AI systems, as they can operate outside the framework of traditional privacy principles.
- According to Puneet Kapoor, Executive Vice President at Kotak Mahindra Bank, FSS's Access Control may be achieved using **device history & data and Biometrics,** which are distinctive to each person. A **digital signature** is established with the use of hardware security module (HSM) based data encryption, allowing the system to identify any unidentified login.

- There is a lack of Structured mechanisms for collecting, validating, standardizing, correlating, archiving and distributing AI relevant data affects the efficacy of a fraud detection AI systems.
- By comparing Indian, American, Nordic and Singaporean banks, it was discovered that Indian banks—both public and private—are still in the **nascent stages** of using artificial intelligence, with few algorithms on user behavior patterns and data to be fed into the system, as well as Natural Language Processors. The implementation of rule-based algorithms and deep machine learning algorithms with a big amount of data already in the system in the American and Nordic banks is far more advanced than that of India. Yet, India is one of the fast growing country in implementation of AI in this subject matter.

XII. RECOMMENDATION

- In India, there has been a trend of high reliance on foreign AI & ML algorithm platform suppliers. To reduce this reliance and create new algorithms for fraud detection, the government, public and private banks, angel investors, and FDI should support burgeoning unicorns and fintech businesses.

- Use explainable AI methods that allow for transparency and accountability in the fraud detection process. This can help build trust with customers and regulators and ensure that the algorithms are making fair and ethical decisions.

- Implement a multi-layered fraud detection system that utilizes both rule-based systems and machine learning algorithms. This can help identify suspicious transactions based on predefined rules and also detect new patterns of fraud using machine learning algorithms.

- RBI has to play a proactive and more dynamic role in framing regulations to balance the business interest of banks and at the same time ensure customer privacy and information protection.

XIII. CONCLUSION

Based on the research findings, it can be concluded that AI has immense potential in the Indian banking sector, especially in fraud detection and prevention. The implementation of AI-based fraud detection systems can help banks to identify fraudulent activities in real-time and prevent losses. Several initiatives have been taken by Indian banks to find innovative AI based solutions for fraud detection via startup engagement programs, the RBI has proposed the Early Warning Signal framework (EWS) to detect possible loan defaults and mitigating potential frauds which shows a positive trend towards development and implementation of efficient fraud detection systems. However, there are challenges that need to be addressed, such as data privacy and security concerns, lack of skilled manpower, and high implementation costs. Overall, the adoption of AI can bring significant benefits to the Indian banking sector, and it is recommended that banks invest in AI-based solutions to stay competitive in the market.

Bibliography

Btoush, E., Zhou, X., Gururaian, R., Chan, K., & Tao, X. (2021). A Survey on Credit Card Fraud Detection Techniques in Banking Industry for Cyber Security. *2021 8th International Conference on Behavioral and Social Computing (BESC).* Doha, Qatar: Institute of Electrical and Electronics Engineer. doi:10.1109/BESC53957.2021.9635559

Vorobyev, I., & Krivitskaya, A. (2022, September). Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models. *Computers & Security, 120*. doi:https://doi.org/10.1016/j.cose.2022.102786

Alhaddad, M. M. (2018). Artificial Intelligence in Banking Industry: A Review on Fraud Detection, Credit Management, and Document Processing. *Researchberg Review of Science and Technology, 2*(3), 25-46. From https://researchberg.com/index.php/rrst/article/view/37

Bank of Baroda to set up AI center to tackle financial frauds. (2019, March 4th). From Money Control: https://www.moneycontrol.com/news/business/companies/bank-of-baroda-to-set-up-ai-center-to-tackle-financial-frauds-3606991.html

Kochhar, K., Purohit , H., & Chutani , R. (2019). The Rise of Artificial Intelligence in Banking Sector. *THE 5th International Conference on Educational Research and Practice(ICERP)*, (pp. 142-158). PUTRAJAYA, MALAYSIA. From https://spel3.upm.edu.my/max/dokumen/ICERP_ICERP_2019_-_PROCEEDINGS_(REVISED)_compressed.pdf#page=142

Kurt, S., Alexander, M., & Alexand, D. (2019). Fraud Detection in Payment Transactions: Overview of Existing Approaches and Usage of Instant Payments. *20*, 72. From https://metsearch.cardiffmet.ac.uk/permalink/44WHELF_CMU/1roeqsq/cdi_swepub_primary_oai_DiVA_org_hj_47495

Soni, V. D. (2019). ROLE OF ARTIFICIAL INTELLIGENCE IN COMBATING CYBER THREATS IN. *International Engineering Journal of Research and Development, 4*(1), 3-6. doi:https://doi.org/10.17605/OSF.IO/JYPGX

Vijai, D. C. (2019, April). ARTIFICIAL INTELLIGENCE IN INDIAN BANKING SECTOR: CHALLENGES AND OPPORTUNITIES. *International Journal of Advanced Research , 7*(5), 1581-1587. doi:10.21474/IJAR01/8987

THE ASIAN BANKER. (2019, 7 26). *HDFC Bank embarking on AI and machine learning initiatives to detect fraud.* Retrieved from www.theasianbanker.com: https://www.theasianbanker.com/updates-and-articles/hdfc-bank-embarking-on-ai-and-machine-learning-initiatives-to-detect-fraud

Tarantola, A. (2022, 9 25). *Hitting the Books: How Southeast Asia's largest bank uses AI to fight financial fraud.* Retrieved from https://www.engadget.com/hitting-the-books-working-with-ai-davenport-miller-mit-press-150016191.html#:~:text=DBS%20Bank%3A%20AI%2DDriven%20Transaction%20Surveillance&text=DBS%20Bank%2C%20the%20largest%20bank,financial%20crime%20detection%20and%20preventio

ICICI Bank. (2021). ICICI Bank deploys AI-based fraud detection system. Retrieved from https://www.icicibank.com/aboutus/article.page?identifier=news-icici-bank-deploys-ai-based-fraud-detection-system-2021

Bhati, S. (2021). Use of AI in Fraud Detection in Indian Banking. Retrieved from https://www.analyticsinsight.net/use-of-ai-in-fraud-detection-in-indian-banking/

Sankhyana consultancy services. (n.d.). Retrieved from sankhyana.com: https://sankhyana.com/blog/AI-in-Banking-How-AI-is-transforming-Banking-Sector-\

Citibank. (2021). Fraud Detection. Retrieved from https://www.citibank.com/commercial-bank/solutions/treasury-and-trade-solutions/fraud-detection/

Suparna, B., Renny, T., Shwaitang, S., Violet, C., & Brant, C. (2020, 9 19). *AI-bank of the future: Can banks meet the AI challenge?* Retrieved from mckinsey.com: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge

Mejia, N. (2019, 10 14). *Artificial Intelligence at Citibank – Current Initiatives.* Retrieved from emerj.com: https://emerj.com/ai-sector-overviews/ai-at-citi/

Cukier, K. (2020). AI for Fraud Detection: Benefits and Challenges. Retrieved from https://emerj.com/ai-sector-overviews/ai-for-fraud-detection-benefits-and-challenges/

Chitra, R. (2016, August 27th). *Banks use artificial intelligence to prevent frauds*. From Times of India: https://timesofindia.indiatimes.com/business/india-business/banks-use-artificial-intelligence-to-prevent-frauds/articleshow/53881247.cms

Columbus, L. (2019, August 01st). AI Is Predicting The Future Of Online Fraud Detection. *Forbes*. From https://www.forbes.com/sites/louiscolumbus/2019/08/01/ai-is-predicting-the-future-of-online-fraud-detection/?sh=f76bb7474f51

Donahue, J. (2017). Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real Time. *TERADATA PARTNERS CONFERENCE.* Anaheim, California. From https://www.teradata.com/Press-Releases/2017/Danske-Bank-and-Teradata-Implement-AI

Money Control. (2019, March 4th). *Bank of Baroda to set up AI center to tackle financial frauds*. From Money Control: https://www.moneycontrol.com/news/business/companies/bank-of-baroda-to-set-up-ai-center-to-tackle-financial-frauds-3606991.html

Rathore, M. (2022, September 29th). *Status of online banking in India in 2020*. From Statista: https://www.statista.com/statistics/1249581/india-status-of-online-banking-adoptio/

Vijai, D. C. (2019, April). ARTIFICIAL INTELLIGENCE IN INDIAN BANKING SECTOR: CHALLENGES AND OPPORTUNITIES. *International Journal of Advanced Research , 7*(5), 1581-1587. doi:10.21474/IJAR01/8987