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. According to a survey conducted in 2022 by PWC and FICCI, the Indian banking industry is at the forefront of deploying and embracing all new 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 considerable advancements in the Indian banking sector and the incorporation of AI into its system, it presently lacks the proper tools and technologies, as well as strong regulatory rules and a qualified workforce, to detect signs of fraud. 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.

The study attempts to investigate numerous frauds committed in the banking sector and the present difficulties in the methods currently used for fraud detection in India through analysis and data from various sources. 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. KEYWORDS

Artificial intelligence, Fraud detection, modern technology, Machine learning, Banking industry

III. INTRODUCTION

a) Classification of Frauds:

In order to preserve consistency in reporting and in accordance with the provisions of the Indian Penal Code, 1986, the RBI published a Master Directive in 2016 with the following guidelines to report as "Fraud":

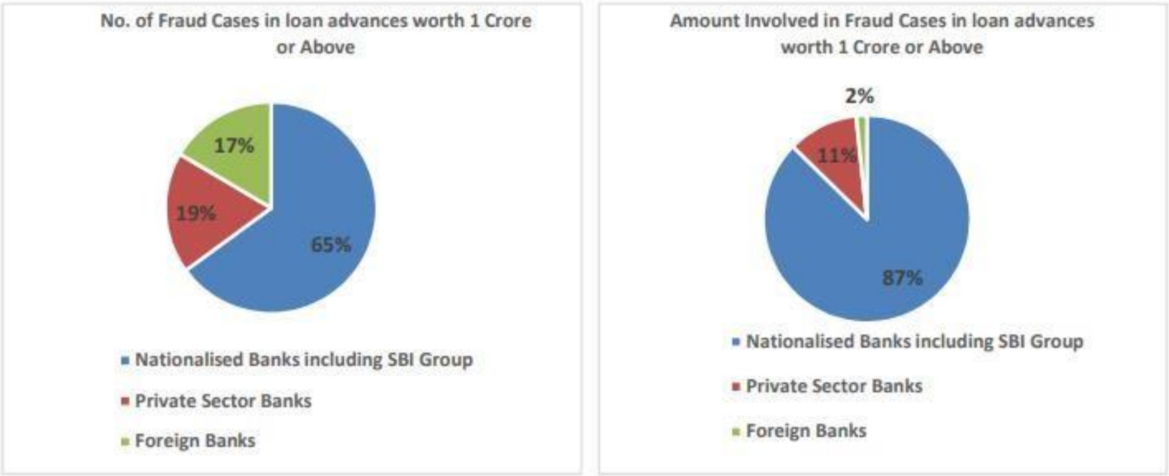
- Theft and treasonous violation of trust.
- Fraudulent encashment through the use of counterfeit documents, falsified accounts, or other types of accounting manipulation, as well as property conversion.
- Unauthorized credit lines are made available as a form of payment or for illicit satisfaction.
- Cash flow problems.
- Dishonesty and forgery.
- Fraudulent foreign exchange transactions.
- Any other form of fraud not covered by the aforementioned categories.

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. An indication of poor corporate governance is the incidence of high-value bank loans as a result of collaboration between corporate entities and top bank officials. 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).

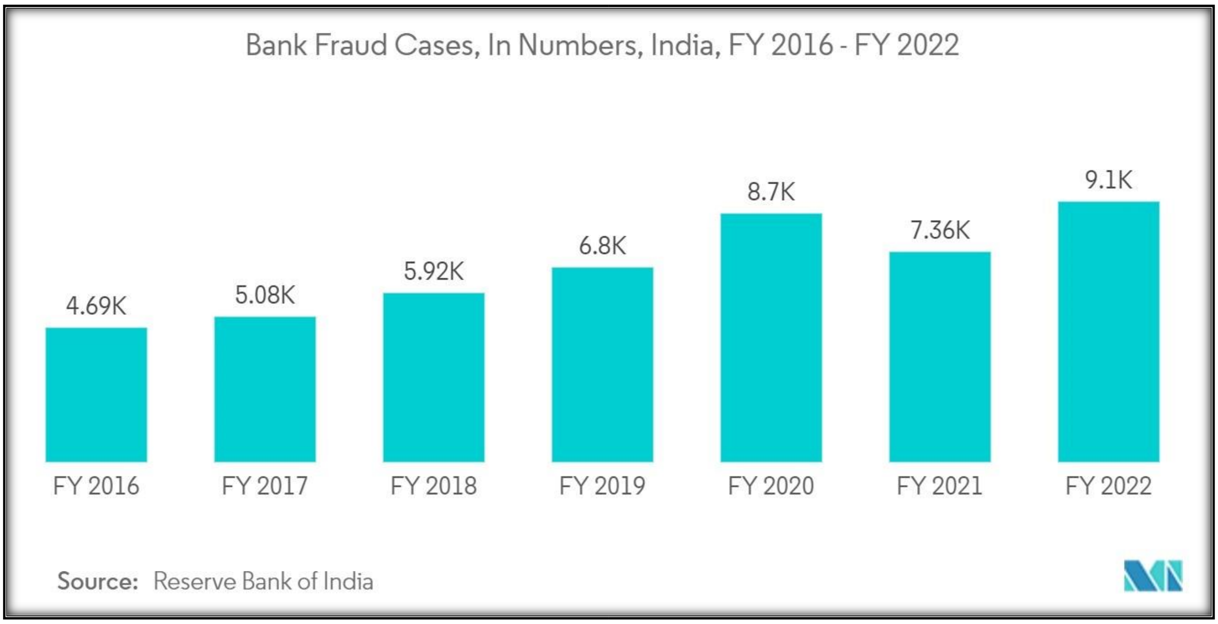
Chart 1. Proportion of Banks in number of fraud incidents and amount involved in Deposit-frauds

- **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**

Large-scale loan advance frauds are challenging to pull off, and they frequently start with bank workers collaborating with customers and occasionally even with agents of third parties like attorneys 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. Staff personnel who are unaware of correct procedures and warning indicators they ought to be aware of, also contribute to fraud as well. The biggest reason for technology-related fraud is staff members who don't follow set standard procedures and practices.



Source: Reserve Bank of India

Chart 2. Bank Fraud cases from FY 2016-2022

IV. 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 labor 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.

V. 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.

VI. LITERATURE REVIEW

Along with raising credit scores, enhancing customer service, and lowering the risk of falling victim to scams, AI has been playing a crucial role in detecting fraud. 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. The banking industry has a difficult time preventing credit card fraud brought on by a stolen, misplaced, or fake card because of the volume of financial transactions involved. The difficulty for AI and ML in identifying such fraud is due to the skewness of credit card fraud sets of data, which results from the fact that the number of forged payments is far lower than the number of genuine transactions. Systems for detecting credit card fraud must be highly flexible in the real world as well. The speed of the computer system must be sufficient to accommodate the massive amount of data generated each 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 banking fraud prevention systems based on rule induction in networked tree-based models," addresses the issue of false positives in bank payments, critiquing the present fraud detection method and its inefficiency. They strive to raise productivity of bank fraud detection measures by implementing a 'rules induction technique' framework in which new rules are generated by implementing tree-based algorithms like Decision Tree and Random Forest, which seek to detect instances that are currently misclassified as fraud. Over first part of the year, the framework was put to the test in a real bank's fraud monitoring system. The regulations created using this framework have been shown to be sufficiently effective and to have a definite commercial impact.
(Vorobyev & Krivitskaya, 2022)

There are various elements of web-based banking frauds, including how they pose a serious challenge to current fraud detection techniques and data mining models and how, when directly implemented in online banking fraud detection, they exhibit low efficiency and/or accuracy. Additionally, they provide a framework for effectively detecting online banking fraud that unifies several sophisticated data mining techniques and creates appropriate resources. They draw the conclusion that experiments carried out to evaluate the effectiveness of the system in question were not only successful but also more accurate and produced fewer alerts than expected. **(Wei et al., 2012)**

The study focuses on the increase in fraudulent use of credit cards as it becomes more and more popular for both regular and online transactions due to the rapid development of electronic commerce technologies. It provides an analysis of numerous modern approaches based on artificial intelligence used in credit card fraud detection mechanisms, including data mining, neural networks, Bayesian networks, fuzzy logic, artificial immune systems, the K-closest neighbor algorithm, support vector machines, decision trees, fuzzy logic-based systems, ML, genetic programming, sequence alignment and an artificial immune system. **(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 steadfastly incorporating AI-enabled technologies in their business operations in recent years. A significant number of commercial and industrial banks worldwide have adopted AI and its allied technologies for managing customer and back-office related tasks, but it’s not sufficient (BFSI, 2019).

The most advanced technology is artificial intelligence (AI), which can analyze a person's past spending habits and behavior towards various transactions and spot abnormalities. AI may also understand data based on past experience if it notices an abnormality in routine transactions and fixes it, the system will learn from the experience and be better able to determine what constitutes fraud and what does not. **(Malali & Gopalakrishnan, 2020)**

Fraud has been a major issue in the financial sector, and fraud detection is one of the most significant fields in the financial services industry where AI systems have excelled. Since AI uses algorithms to analyze trends and predictive modelling to prevent fraudulent transactions, they describe it as being particularly good at spotting trends in real time and helping banks prevent financial fraud. Additionally, they demonstrate the use of advanced deep learning-powered artificial intelligence systems today using the FICO Falcon fraud assessment system, which operates on a neural network shell, and draw the conclusion that fraud detection has advanced significantly and is anticipated to do so in the years to come. **(Kaur et al., 2020)**

AI applications have been 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 and ML 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 present state of AI in each. With the banking sector in mind, 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 Block chain technologies into practice. Additionally, it has been stated that anomaly detection can increase the precision of preventing money laundering and detection of credit card fraud. (Vijai, 2019)

VII. RESEARCH GAP

- The study on the use of AI and ML in fraud detection in the banking sector 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.

VIII. 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:** Elsevier's Scopus database contains citations to and abstracts of works that have undergone peer review. It is the biggest abstracts and citation database for scientific publications with peer review, books, and conference proceedings.
- **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 20122022 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.

IX. 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.

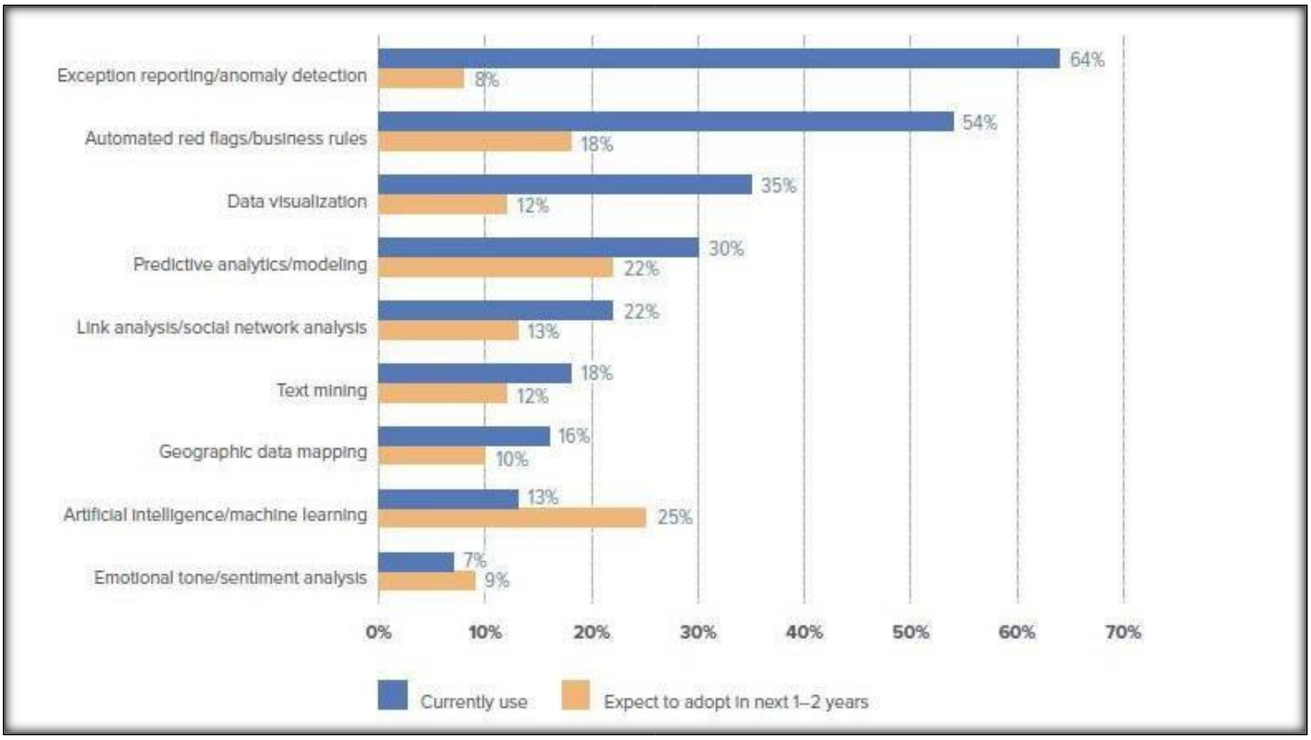


Chart 3. Fraud identification techniques used in AI by Banks

X. 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. According to a poll conducted in 2022 by PWC and FICCI, the banking industry in India is in the forefront of implementing and embracing all new 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.

According to Markets, the Fraud Identification and Prevention Market will increase at a CAGR of 26.7% from $ 19.5 billion in 2018 to $ 63.5 billion by 2023. Increased revenue losses for businesses as a result of increased fraudulent attacks, rising use of digital payments across all verticals, and the sophistication of cyberattacks globally are the main drivers anticipated to drive the FDP market.

a) HDFC & DBS BANK

HDFC has invested in operational centers that are staffed around-the-clock to continuously monitor and analyze traffic in real-time while providing prompt issue response. Along with starting a startup engagement programmed for fintech startups, they have also partnered with top AI suppliers to assist detect frauds more readily, especially complex frauds that are difficult to detect using conventional safety and event monitoring techniques. The difficulties HDFC encounters include the potential for hackers to launch distributed denial-of-service (DDoS) attacks that render the infrastructure not available for an extended period of time, worries about API security, and the requirement for the correct people and processes to develop the APIs.

The biggest financial institution in Singapore and Southeast Asia, DBS Bank, uses AI to evaluate alerts produced by a rule-based system in its "transaction surveillance" function. The standards assess transactional information from a variety of bank systems, encompassing those for customers, assets, institutional in nature, and payments banking. All of these transactions are screened using a rule-based system, and the rules draw attention to transactions that meet requirements related to someone or something that may be involved in transactions that could be used to launder money with the bank. Almost all of the alerts generated by rule-based monitoring systems—up to 98 percent of them—are false positives. The transaction in some way triggers a rule, which results in the transaction being marked and added to the alert list. However, a follow-up investigation by a human analyst indicates that the transaction that triggered the alarm is otherwise, suspicious.

DBS began a project a few years ago to combine the current rule-based screening system with the most recent generation of AI/ML capabilities. The combination would allow the bank to order all of the rule-based system's alerts based on the amount of suspicion indicated by a numerically computed likelihood score. The machine learning algorithm was trained to identify suspicious and fraudulent scenarios using both recent and old data and results.

In order to help the examination of flagged transactions, DBS also created additional new capabilities, such as the Network Link Analytics tool for spotting suspicious linkages and transactions involving many parties. Money transactions can be visualized as a network graph, with the parties involved as nodes and any interactions between them as links.

After a thorough study of these two banks, it was observed that HDFC has teamed up with leading vendors in AI can easily identify frauds, especially sophisticated scams that are undetectable by conventional surveillance and event monitoring techniques, 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 began a project to combine the current rule-based screening system with the most recent wave of AI/ML capabilities. This gave the bank the opportunity to order all of the rule-based system's alerts based on a numerically derived likelihood score that indicated the degree of suspicion. It already had a feature called "transaction surveillance" where qualified staff members kept an eye on and oversaw both their old and new artificial intelligence (AI) systems.

b) ICICI & CITIBANK

One of the major private sector banks in India, ICICI Bank, has put in place a powered by AI identification system to spot and stop scams in real time. The technology evaluates consumer behavior using machine learning techniques, looking for any irregularities that would point to fraudulent conduct. One advantage of the AI system used by ICICI Bank is its capacity to spot suspected fraud in actual time, enabling the organization to take prompt action to stop losses. Additionally, by lowering the amount of false alarms and the requirement for manual intervention, the application of AI has increased the precision of fraud detection.

The efficiency of ICICI Bank's AI driven technology is heavily reliant on the caliber and volume of available data as well as the possibility of algorithmic bias, which is one of the system's problems. The bank must continuously gather and analyze vast volumes of consumer data to make sure the software is as precise as possible. Furthermore, the AI system might produce false positives, which would result in pointless inquiries and operational costs.

If the information used to train AI models is biased, this can result in biased predictions and choices. As a result, it is crucial to make sure that the information being utilized for training AI models is impartial and diverse. Finally, to ensure that AI models continue to be successful in identifying novel kinds of fraud and adjusting to shifting fraud patterns, they must be regularly checked and updated.

An AI-powered forgery detection system has been used by Citibank, a foreign bank, to increase fraud detection accuracy and decrease false positives. To find anomalies and trends in consumer behavior that may point to fraudulent activities, the bank uses powerful machine learning and analytics algorithms. The ability of Citibank's AI driven system to examine vast amounts of data enables the bank to spot minor trends that could be overlooked by humans. The method can also lessen false positives, saving the bank time and resources.

When Citibank tried to integrate AI into its fraud-detection systems, there were a number of obstacles. A weak underlying technology and data foundation, an outdated operating model, and a talent strategy were some of the difficulties.

However, to incorporate their AI system for risk control and identifying fraudulent activity in banking, Citibank teamed up with fintech startup Feedzai.

The protection of consumer data's privacy and security is another difficulty for Citibank's AI system. Customers may be concerned about the system's heavy reliance on client data to detect potential fraud. The bank must also guarantee that the artificial intelligence (AI) system is safe and cannot be compromised by cybercriminals.

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 exterior sensor and internal data source 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 Teradata company, Think Big Analytics, 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.

The engine employs machine learning to evaluate tens of thousands of concealed factors and grade millions of transactions made via the internet in real-time, delivering actionable knowledge about genuine and phony fraudulent activity. By significantly reducing the cost of analyzing false-positives, Danske Bank improves its efficiency as a whole and is now ready for expansion. **(Donahue, 2017)**

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

The most recent research initiatives shed light on the reasons why artificial intelligence (AI) is going to be the future for web fraud detection. According to the Association of Certified Fraud Examiners' (ACFE) first Anti-Fraud Technology Benchmarking Report, businesses expect to triple their investment in AI and machine learning by 2021 to combat online fraud. Only 13% of businesses currently use machine learning and artificial intelligence to detect and deter fraud, according to the ACFE survey. The study found that another 25%, or about a 200% increase, intend to use such innovations in the upcoming year or two. Predictive data analysis and modelling will likely be employed to combat fraud in the following two years, according to the ACFE report, followed by machine learning and artificial intelligence technology.

XII. 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. Currently, there are 3.4 crore active digital channel users; as a result of the COVID-19 pandemic, this number nearly tripled to 7.6 crores in 2020–2021. **(Rathore, 2022)**
- The privacy policies introduced by the RBI pose a challenge in regulating AI systems because they have the ability to function outside the bounds of conventional privacy norms.
- 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.
- The effectiveness of fraud detection AI systems is impacted by inadequate systems for gathering, validating, standardizing, correlating, archiving, and disseminating AI-relevant data.
- 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.

XIII. 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.
- In order to strike a balance between the economic interests of banks and the protection of client privacy and information, the RBI must take a more proactive and active role in formulating regulations.

XIV. CONCLUSION

From research findings, it can be summarized that AI has immense potential in the Indian banking sector, especially in fraud detection and prevention. The implementation of AI-based 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 privacy, safety and security concerns, lack of skilled manpower, and high implementation costs. Overall, the adoption of AI can bring significant benefits to the Indian banking industry, and it is recommended that banks invest in AI-based solutions to stay competitive in the market.

XV. BIBLOGRAPHY

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-thebooks-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-bankdeploys-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/indiabusiness/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-ofonline-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