

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

دور الذكاء الاصطناعي في الحد من الاحتيال المصرفي وتعزيز الأمن السيبراني في القطاع المصرفي
-إشارة إلى تجربة بنك بنجاب الحكومي (الهند)-

Abassi Abderraouf ¹, Bouzerb Khayreddine ²

¹ University of Jijel, Faculty of Economic, Commercial, and Management Sciences (Algeria),
abderraouf.abassi@univ-jijel.dz

² University of Jijel, Faculty of Economic, Commercial, and Management Sciences (Algeria),
K.bouzerb@univ-jijel.dz

Received: 12/01/2026

Accepted: 10/06/2026

Published: 12/06/2026

Abstract:

This descriptive-analytical study aimed to highlight the importance of adopting artificial intelligence applications to combat fraud and enhance cybersecurity in banks. This study reviewed the Indian experience in this field, particularly the case of the Punjab State Bank, which was exposed to a fraud in 2018. This fraud significantly impacted the bank and extended to other banks and markets.

This study reached a number of conclusions that highlight the significant importance of artificial intelligence in detecting fraud, which is experiencing increasing levels worldwide. It recommended the need to enhance monitoring and auditing using artificial intelligence mechanisms to reduce fraud and enhance financial stability.

Keywords: Artificial Intelligence; Automation; Robotics; Fraud; Cybersecurity.

JEL Classification Codes: G21, O33.

ملخص:

هدفت هذه الدراسة ضمن إطار وصفي تحليلي إلى إبراز أهمية تبني تطبيقات الذكاء الاصطناعي في مواجهة الاحتيال وتعزيز الأمن السيبراني في البنوك، وهذا من خلال استعراض التجربة الهندية في هذا المجال وبالأخص حالة بنك بنجاب الحكومي الذي تعرض لعملية احتيال خلال عام 2018، هذه العملية أثرت بشكل كبير على البنك وأمتد تأثيرها إلى بنوك وأسواق أخرى.

من خلال هذه الدراسة تم التوصل إلى جملة من النتائج تبرز الأهمية الكبيرة التي يحظى بها الذكاء الاصطناعي في الكشف عن الاحتيال الذي يعرف مستويات متزايدة في العالم، وتمت التوصية بضرورة العمل على تعزيز المراقبة والتدقيق بالاعتماد على آليات الذكاء الاصطناعي من أجل الحد من حالات الاحتيال وتعزيز الاستقرار المالي.

كلمات مفتاحية: ذكاء الاصطناعي، أتمتة، روبوتات، احتيال، أمن السيبراني.

تصنيفات JEL: G21، O33.

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

INTRODUCTION:

Over recent decades, numerous technologies and innovations have dominated the global economy, with technology becoming an indispensable necessity in the modern era as a fundamental component of the business environment. It has facilitated the creation of new methods and approaches across various fields. Because of the rapid and continuous advancement in these technologies, artificial intelligence (AI) programs based on sophisticated techniques have emerged, enhancing human functions. Consequently, institutions worldwide are increasingly striving to adopt these digital technologies to boost their competitiveness and attract a broader customer base.

Within the context of banks' efforts to strengthen cybersecurity and maintain customer trust amid intense competition in the banking sector, artificial intelligence has emerged as a key technology to combat fraud and cyberattacks. Supported by numerous governmental initiatives, many banks have intensified their efforts and research to develop intelligent systems and programs that enable early fraud detection and help banks establish a strong presence in a digital world where geographical boundaries have diminished, making every individual a potential customer.

Research Problematic:

The Indian banking system ranks among the most significant globally, with total assets reaching USD 3,126.3 billion according to 2024 data (IBEF, 2025), placing it fourth worldwide after China, the United States, and Japan. However, this scale conceals numerous fraud-related challenges, which India has sought to address by encouraging the adoption of AI-based mechanisms. From this perspective, the following research question arises:

What Role Can the Adoption of Artificial Intelligence Play in Reducing Banking Fraud and Enhancing Cybersecurity ?

Research Aims:

This study aims to achieve the following objectives :

- to present the various cybersecurity threats at the banking level and explain how AI is employed to mitigate these threats;
- to analyze the Indian experience in using AI to combat banking fraud, specifically focusing on the case of the Punjab Government Bank.

Study Significance:

The importance of this study is highlighted by several factors. Firstly, the increasing scale and impact of banking fraud on global banking systems, with losses attributed to banking fraud exceeding \$1.03 trillion worldwide within a single year (Feedzai, 2024). Secondly, the expanding market size of artificial intelligence (AI) in the global banking sector, which was valued at \$26.23 billion in 2024 and is projected to reach approximately \$379.41 billion by 2034 (Shivani & Aditi, 2025)

Methodology and Data Sources:

The study adopts a descriptive-analytical methodology to collect and describe the various concepts under consideration and to analyze the use of AI in reducing fraud and enhancing cyber security within the Indian banking sector in general, and the Punjab Government Bank in particular. Regarding data sources, reliance was placed on books, academic journals,

conferences, and symposiums, in addition to various statistics, reports, and relevant regulations pertaining to the bank under study.

Literary Review:

Literary Review on the role of AI in mitigating fraud and strengthening cybersecurity represents a growing field, as financial institutions strive to adopt advanced technologies to combat digital threats. Among the most prominent studies in this area:

- **Study Andreas Svoboda (2023):** This study aimed to develop a comprehensive overview of artificial intelligence (AI) and provided insights into the impact of AI adoption within the banking sector in India. As a descriptive study, data were collected from a variety of sources, including journals, periodicals, and online platforms such as websites. The findings indicate that AI enables financial institutions to enhance customer service capabilities, improve financial performance, and maintain competitiveness in an increasingly digital landscape.

- **Study Bhavya & Kehaan (2023):** Conducted within an analytical framework, this study focused on highlighting the role of AI in fraud detection and its implementation in Indian banks compared to foreign banks. The study concluded that AI holds significant potential in the Indian banking sector, particularly in fraud detection and prevention. Implementing AI-based detection systems can assist banks in identifying fraudulent activities in real time and mitigating losses. However, several challenges remain to be addressed.

- **Study Chittimalla Bhargavi & Sravanthi (2023):** This study aimed to examine how digital technologies are utilized in banking fraud detection, including the use of machine learning algorithms, and explored how stakeholders can protect themselves from banking fraud. The results emphasize the importance of educating both employees and customers about phishing attacks and social engineering threats, as well as alerting customers through notifications whenever suspicious activity occurs within online banking systems. Additionally, the study recommends that banks integrate fraud monitoring systems and conduct daily manual reviews of reports.

- **Study Bukhtueva (2024):** This study focused on highlighting the role of AI in financial risk management and fraud detection by comparing traditional methods with AI techniques in terms of their ability to process large volumes of data, recognize complex patterns, and adapt to market changes. Successful AI applications within the financial sector were illustrated through case examples from various companies. The findings indicate that AI substantially enhances operational efficiency and security in financial institutions.

Points of Convergence and Divergence Between the Current Study and Previous Research: The current study aligns with previous research in addressing banking fraud and cybercrime as critical risks facing the banking sector, especially amid rapid technological advancements. However, it differs in terms of its focus, concentrating specifically on one of the major public sector banks in India that experienced a significant fraud scandal in 2018. This incident prompted the bank to pursue advanced AI-driven technologies as a strategic response to prevent future fraudulent activities.

1- The General Framework of Artificial Intelligence (AI) and Its Applications in the Banking Sector:

The implementation of artificial intelligence accelerates corporate transformation, making organizations more advanced and fostering their continuous development. This section

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

will address various theoretical aspects related to artificial intelligence (Medvedeva & Khvesko, 2021, p. 355).

1-1 Definition of Artificial Intelligence: There is no single, definitive definition of artificial intelligence due to the complexity of the field and its intersection with numerous concepts. Among the definitions proposed are the following:

- According to the World Bank, artificial intelligence comprises a set of systems and technologies designed to simulate human capabilities such as learning, reasoning, decision-making, pattern recognition, and interaction with the environment. AI is employed in a broad range of applications, including enhancing public service delivery, improving efficiency, and implementing policies, particularly in sectors such as health and finance (World Bank, 2025).
- The Organization for Economic Co-operation and Development (OECD) says that artificial intelligence is a machine-based system that can figure out how to make predictions, content, recommendations, or decisions that could affect real or virtual environments based on the inputs it gets. Different AI systems are built to work with different levels of autonomy and adaptability after they are put into use (Russel, Perset, & Grobelnik, 2023).

Based on the above, AI can be defined as the development of systems capable of emulating human intelligence across multiple domains by processing data and making intelligent decisions based on the input information. Its applications are expanding across diverse sectors, including financial services, where it contributes to enhancing efficiency and reducing costs through process automation and fraud detection.

1-2 Characteristics of Artificial Intelligence: Artificial intelligence is characterized by several features, which are outlined as follows (VirtuBox, 2024).

- Learning Ability: AI does not require explicit instructions for every task; instead, it utilizes machine learning algorithms to process information, identify patterns, and make decisions.
- Problem Solving: AI possesses the capability to solve complex problems by leveraging algorithms and data to analyze issues and provide effective solutions, often more rapidly than humans.
- Reasoning: Artificial intelligence can make rational decisions based on the data it possesses, employing rules and logic to draw conclusions.
- Perception: AI utilizes sensors and data to understand its environment, much like humans rely on their senses.
- Adaptability: AI systems evolve and adjust to new information or changes in their environment without the need for reprogramming.
- Automation: AI completes tasks autonomously without human intervention, enhancing speed and reducing errors.
- Data Handling: AI's ability to process vast amounts of data is remarkable; it can store, manage, and analyze information rapidly and accurately beyond human capabilities.
- Natural Language Processing: This capability enables AI to interact with humans in a manner that facilitates easier communication between people and machines.

1-3 Applications of Artificial Intelligence in the Banking Sector: AI technology is progressively gaining a significant role within the financial sector. The following are the most important uses of artificial intelligence in the banking sector : (Garifullova & Khametshina, 2024, p. 111).

- **Credit Scoring Technology :** Credit bureaus collect and transfer borrower data from all banks, microfinance institutions, credit cooperatives, and investment platforms.
- **Voice Assistants and Chatbots:** Banks deploy voice assistants and chatbots to improve customer service quality, reduce operational costs, automate daily tasks, and resolve customer issues.
- **Fraud Prevention and Financial Monitoring:** Banks implement fraud detection and financial monitoring systems to ensure regulatory compliance, while collecting and analyzing customer data to guarantee security and privacy.
- **ATM Services:** Financial institutions use ATMs for customer service, along with online management tools, software updates, system diagnostics, and video surveillance to monitor ATM performance.

1-4 Challenges of Integrating Artificial Intelligence in the Banking Sector: The adoption of AI technology faces numerous challenges that may hinder rapid growth and sustainable development of the banking sector. Among these challenges are the following (Ghandour, 2021, p. 1585).

- The obsolescence of certain skills: AI may alter the nature of existing job roles and lead to the disappearance of some skills, potentially resulting in job losses. Consequently, ensuring user acceptance of AI technologies in banks could represent a significant challenge.
- Privacy violations: Most banking AI systems rely on the collection and analysis of vast amounts of customer data, including demographic information, spending patterns, biometric data, credit and debit card details, and social media profiles. As a result, consumer privacy and security become vulnerable when AI is deployed.
- Loss of creativity and flexibility: Relying too much on AI to make decisions and solve problems may make employees less creative and flexible.
- Potential digital divide: Customers lacking access to modern personal devices (such as computers, smartphones, or tablets), internet connectivity, or technical skills may be unable to benefit from banking AI systems.

2- Application of Artificial Intelligence in Detecting Banking Fraud and Enhancing Cybersecurity:

The Merriam-Webster Dictionary says that "cybersecurity" is the steps taken to keep a computer or computer system (like those on the internet) safe from being accessed or attacked by someone who shouldn't be able to (Merriam - Webster Dictionary, 2020). Cybersecurity also includes keeping hardware, software, and data on internet-connected systems safe from cyberattacks. The main goal of this field is to work together to make people, processes, and technologies safer and less likely to be attacked. It includes things like working together with other countries and using computer networks for operations (Kamalov & Mamatjonov , 2024, p. 22).

2-1 Concept and Importance of Financial Cybersecurity: Financial cybersecurity is a specialized branch of information security that involves safeguarding data and processes from digital threats. It emerged as a response to the increasing risks associated with the active use of electronic payments, online banking, and mobile applications. Its core mission is to protect financial systems, customer data, and transaction processes from various attacks and fraudulent activities (Sledneva & Kuvaldina, 2024, p. 24).

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

The financial sector is among the most vulnerable to cyber risks, accounting for nearly one-fifth of global cyber incidents over the past two decades, with banks being the primary targets, followed by insurance companies and asset managers (IMF, 2024, p. 80). Because cyberattacks can have very bad effects, cybersecurity is very important in the financial sector. Data breaches cost money, hurt your reputation, and can get you in trouble with the law. Cyberattacks can also stop the delivery of financial services, which hurts both customers and the economy as a whole (Krakowczyk, 2024). For instance, reports prepared by experts from the Solar Group revealed that Russia recorded approximately 6,800 cyber incidents in the financial-credit sector in 2023, representing a 25% increase and indicating heightened activity by malicious actors seeking to exploit vulnerabilities within financial systems (Solar, 2023, p. 06).

According to a specialized study conducted in 2019, the average cost of cybercrime per company in the financial services sector exceeds \$18 million, which is approximately 40% higher than the average cost in other sectors. This is illustrated in the following table:

Table (01): Cybercrime Costs across Sectors in 2019 (in million \$)

Sector	Cost (%)	Sector	Cost (%)	Sector	Cost (%)
Financial Services	19	Energy	14	Life Sciences	11
Utilities	18	Government Sector	14	Telecommunications & Media	11
Software	16	Consumer Goods	12	Travel	8.2
Automotive Industry	16	Healthcare	12	Other Public Sectors	7.9
Advanced Technology	15	Retail	11	Average	13

Source: Prepared by the researchers based on (Accenture, 2019).

Within the same context, a study by the International Monetary Fund indicated that financial institutions have incurred direct losses totaling approximately 12 billion US dollars since 2004, including 2.5 billion dollars since 2020, with these attacks predominantly concentrated in developed countries (IMF, 2024, p. 80).

This underscores the extensive use of artificial intelligence in cybersecurity, where AI is applied across various domains such as creditworthiness assessment, fraud detection, and intrusion recognition (Alrafi & Mishra, 2024, p. 09).

2-2 Forms of Financial Cybersecurity Threats: Financial cybersecurity threats manifest in several key forms, notably (Dawodu, Omotosho, Akindote, Adegbite, & Ewuga, December 2023, p. 226).

- Ransomware is a type of malware that locks up the victim's data or systems and asks for money to unlock it. Ransomware attacks can hurt the reputation of financial institutions, threaten the privacy of their data, and stop them from doing business.

- Phishing is a type of social engineering attack in which fake emails or messages that look like they came from trusted sources, like banks or government agencies, are sent. The goal is to trick

people into clicking on harmful links or giving out private information. Phishing attacks can steal your identity, take over your account, commit fraud, or leak your data.

- Denial-of-Service (DoS) Attacks: These attacks target bank websites or electronic services by overwhelming them with an excessive volume of requests or traffic, causing slowdowns or service outages for legitimate users. DoS attacks may be used for extortion, business disruption, or as a diversion to mask other attacks.

- Data Breaches: These incidents involve unauthorized access to bank data through hacking, insider threats, or physical theft. Data breaches can expose confidential information such as customer records, account details, transaction histories, or intellectual property to hackers, criminals, competitors, or the public.

- Advanced Persistent Threats (APTs): These are sophisticated, covert attacks characterized by prolonged infiltration into a bank's network or systems by adversaries with significant resources and strong motivations, such as nation-states, terrorist groups, or cybercriminal organizations. APTs employ a variety of tactics including phishing, malware, and insider collusion.

- Banking Fraud: Attempts to exploit banking systems or technologies to gain unauthorized access to accounts or data for financial gain, taking various forms, including (Kumar, Govardhan, Kaushik, Harshith, & Madhu, 2023, p. 55).

- Payment Fraud: This encompasses a range of fraudulent activities, such as account takeover (where fraudsters obtain victims' passwords and payment information to execute unauthorized purchases) and authorized push payment fraud (where social engineering techniques are used to convince victims to transfer funds).

- Card Fraud: This occurs when a fraudster gains possession of an individual's credit or debit card to make unauthorized purchases, or when they obtain the card data and use it without needing the physical card.

- Merchant Fraud: This refers to fraudulent activities targeting merchants who act as intermediaries between banks and the business sector. Such fraud includes transaction laundering and refund fraud.

2-3 Methods for Achieving Cybersecurity in Banks: Among the proven effective measures for protecting bank assets and maintaining customer trust are the following (Krakowczyk, 2024).

- Use of multi-factor authentication: This adds an extra layer of security by requiring verification through more than one method before allowing access to systems and sensitive data.

- Regular security audits and penetration testing: Checking security systems on a regular basis to find weaknesses.

- Employee Training and Awareness Programs: Teaching employees about the newest cyber threats and how to avoid phishing attacks, social engineering, and other risks that come from people.

- Use of Advanced Encryption Technologies: Using strong encryption to protect data while it is being sent and when it is not being used.

- Network Segmentation: This means breaking up networks into smaller parts to make it less likely that an attack will spread and to keep any breaches that do happen from getting out of control.

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

- Planning for incident response means making and updating plans for how to respond quickly and effectively to possible cyberattacks.
- Working with cybersecurity experts: teaming up with specialized groups to keep an eye on threats and get professional advice on risks and new trends.
- Following industry-specific laws and standards, like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS), to make sure you are following the law and keeping your data safe.

2-4 The Use of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity: AI technologies are fundamental in fraud detection, utilizing advanced algorithms to monitor transaction patterns and identify suspicious activities. This real-time analysis helps prevent fraudulent transactions and safeguard customer accounts (Shah, 2024, p. 722). Key benefits of AI in fraud detection include (Kumar S. , 2024):

- **Rapid Detection:** Speed in processing is one of the most significant advantages of AI and machine learning. By recognizing customer application usage patterns, the system can detect anomalies or unusual behavior in real time. It also outperforms manual methods in efficiency, reducing false positives and allowing specialists more time to focus on complex cases.

- **Higher Accuracy:** AI enables systems to analyze vast volumes of data at high speed and increasing precision. As a result, analytical teams can gain actionable insights more quickly. These technologies also help distinguish between legitimate customers and fraudsters based on input data, verifying the authenticity of payment methods used.

In addition to the above, further benefits of using AI in fraud detection are presented in the following table, which provides a comparative analysis of the effectiveness of AI versus traditional methods in fraud detection.

Table (02): Comparative Analysis of the Effectiveness of Artificial Intelligence and Traditional Methods in Fraud Detection

Criterion	Artificial Intelligence	Traditional Methods
Adaptability	Ability to learn and adapt to new fraud patterns.	Limited adaptability requiring regular rule updates.
False Positives	Lower rate of false positives due to more accurate and detailed analysis in AI systems.	Higher rate of false positives due to reliance on simple rules and manual analysis.
Costs	High initial costs but reduced operational expenses in the long term.	Low initial costs but higher ongoing operational expenses.
Data Requirements	Requires large volumes of high-quality data.	Requires less data but with reduced analytical efficiency.
Scalability Efficiency	High; capable of analyzing large datasets without loss of efficiency.	Low; demands significant resources as data volume increases.

Source: Prepared by the researchers based on (Bukhtueva, 2024, p. 67).

3- The Indian Experience in Adopting Artificial Intelligence to Reduce Fraud in the Banking Sector:

The 1990s marked the true beginning of financial reform in the Indian economy after a prolonged period of economic isolation and centralized control. These reforms were introduced

in response to the economic decline experienced by India at the end of the 1980s, particularly following the energy crisis.

3-1 Overview of AI Implementation in the Indian Banking Sector: India's economy is undergoing rapid transformation driven by artificial intelligence (AI), which is revolutionizing traditional management technologies. The AI industry is projected to be a fast-growing driver of job creation. Currently, there are approximately 400 startups operating in AI and machine learning domains (Radhika, 2024, p. 04). Reflecting its commitment to AI investment, the Indian government doubled its previous allocations for the Digital India initiative in the 2018 Union Budget to \$480 million, supporting the development of digital technologies. This government commitment encompasses extensive investments in research, training, and skill development across AI, big data analytics, robotics, and digital manufacturing.

Within this context, numerous initiatives directly or indirectly impact the banking sector, including the following:

Table (03): Initiatives for AI Implementation in the Indian Banking Sector

Initiative	Content and Objective
Artificial Intelligence Task Force	The team aims to chart a strategic roadmap for the use of artificial intelligence in India. Its members include representatives from the private sector, particularly from banking and financial services. In March 2018, the team released a report identifying ten key areas where AI could play a vital role in India's socio-economic development, with the financial technology industry being one of these core sectors.
Ministry of Electronics and Information Technology Report on Artificial Intelligence	The ministry established several committees to propose a policy framework for artificial intelligence that includes: - AI platforms and data; - Leveraging AI to identify national priorities within key sectors; - Mapping technological capabilities, enabling necessary cross-sector policies, developing and reskilling the workforce, and advancing research and development; - Addressing cybersecurity, safety, as well as legal and ethical issues. - According to the ministry's report, the financial sector is among the fields where AI can be effectively employed. The report identifies fraud detection and the use of predictive analytics to pinpoint non-performing assets and distressed loans as examples of AI applications in the financial sector.
National Strategy for Artificial Intelligence	NITI Aayog was tasked with developing a national artificial intelligence program. In this context, the agency published a discussion paper titled National Strategy for Artificial Intelligence. The "AI for All" strategy is founded on harnessing artificial intelligence to drive inclusive growth, aligning with the government's objective of development for all. The report clearly outlines the necessary government actions and acknowledges that the banking and financial services sector is among the global leaders in AI adoption.

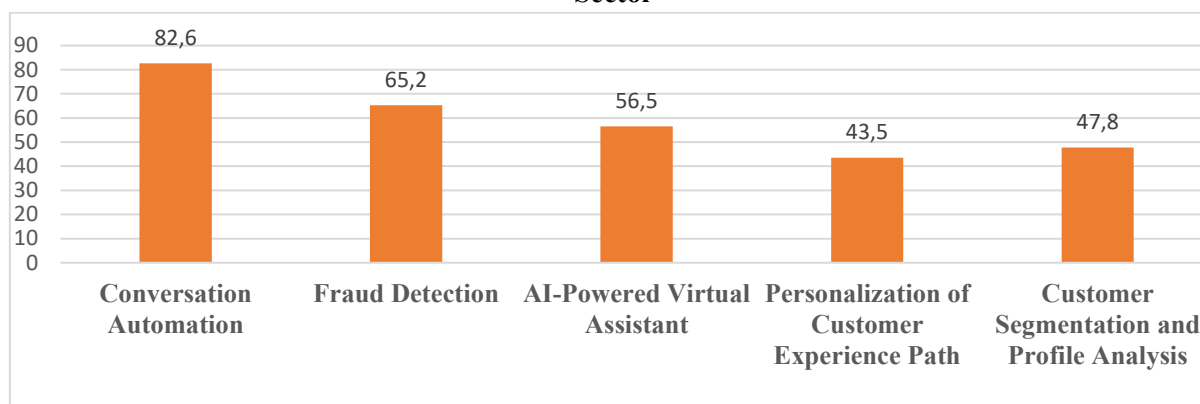
Source: Prepared by the researchers based on (IDRBT and Microsoft India, 2024, pp. 11-12).

In 2024, India launched an initiative aimed at strengthening its innovation ecosystem in the field of artificial intelligence. This initiative includes the development of computing infrastructure, support for startups, and the creation of local tools to ensure safe and ethical AI usage (Aksenova, 2024, p. 101).

Indian businesses use AI to improve quality control and cut costs, which shows how useful AI can be in many ways. Indian banks also use AI to make their fraud detection systems better and their customer service better, which makes the whole process safer and smoother. The following figure shows this:

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

Figure (01): Proportion of Artificial Intelligence Applications in India's Financial Services Sector



Source: Prepared by the researchers based on (Goel, Raut, Kumar, & Sharma, October 2024, p. 221).

The figure highlights that the financial services sector heavily relies on artificial intelligence for automating conversations and detecting fraud. AI is utilized to analyze vast amounts of data in search of suspicious transaction patterns, contributing to early detection and prevention of fraud. According to a report by PwC, the financial sector in India is rapidly adopting AI not only to comply with regulatory requirements but also to gain competitive advantages by enhancing customer experience and operational efficiency (Aksenova, 2024, pp. 100-101).

The following table illustrates the implementation of AI technologies in Indian banks.

Table (04): Implementation of Artificial Intelligence Technologies in Indian Banks

Feature	Indian Banks Implementing the Feature
Chatbots	Bank of Baroda, Andhra Bank, Kotak Mahindra Bank, Canara Bank, City Union Bank, YES Bank, IndusInd Bank, State Bank of India, HDFC Bank, ICICI Bank, Axis Bank
Loan Processing	Axis Bank, State Bank of India, HDFC Bank, ICICI Bank, YES Bank, Federal Bank, South Indian Bank, Maharashtra Bank, Reserve Bank of India, IDFC Bank, IndusInd Bank
Biometric Authentication	State Bank of India, ICICI Bank, Axis Bank, Kotak Mahindra Bank
Fraud Detection	Punjab National Bank (PNB), IDBI Bank, City Union Bank
Transaction Processing	ICICI Bank, Axis Bank, Allahabad Bank, City Union Bank
Document Verification	ICICI Bank, Axis Bank, YES Bank, Bank of Baroda
Risk Monitoring	State Bank of India, Axis Bank, IDBI Bank, HDFC Bank
Sentiment Analysis	State Bank of India, ICICI Bank, Kotak Mahindra Bank
Customer Relationship Management (CRM)	HDFC Bank, IDBI Bank, Allahabad Bank
Customer Segmentation	State Bank of India, HDFC Bank
Sales and Cross-Selling	State Bank of India, HDFC Bank
Credit Evaluation	State Bank of India
International Transfers	ICICI Bank

Source: Prepared by the researchers based on (Bhattacharya & Sinha, 2022, p. 97).

3-2 Legal Framework for Combating Banking Fraud in India: The following overview outlines key legislation (HDFC BANK, 2025):

- **The Banking Regulation Act of 1949:** grants the Reserve Bank of India (RBI) authority to supervise banks and implement measures to prevent fraud. Amendments made in 2020 extended these provisions to cooperative banks as well, ensuring protection across both commercial and cooperative banking institutions.
- **The Prevention of Money Laundering Act (PMLA) of 2002:** mandates banks to maintain detailed transaction records, conduct thorough customer due diligence, and report suspicious activities to the Financial Intelligence Unit, thereby safeguarding against involvement in fraudulent activities.
- **The Information Technology Act of 2000:** Banks have to protect their digital infrastructure and keep customer data safe from breaches, according to the Information Technology Act of 2000. This law also makes cybercrimes like identity theft and phishing illegal, which lowers the chance of losing money.
- **The RBI's Master Circular on Classification and Reporting of Frauds :** divides different kinds of fraud into groups and requires banks to report any incidents that result in losses above a certain level. This makes sure that customers are quickly told about any possible fraud that could affect their accounts.
- **Know Your Customer (KYC):** standards are implemented to verify customer identities, preventing identity theft and the opening of fraudulent accounts. These procedures also ensure the secure handling of personal data and protect against unauthorized access.
- **The Negotiable Instruments Act of 1881:** regulates financial instruments such as checks and promissory notes, providing a legal framework to address fraudulent transactions and offering recourse for customers affected by dishonored or forged instruments.
- **The Bharatiya Nyaya Sanhita Act of 2023:** recognizes "economic offenses," covering crimes such as forgery, currency counterfeiting, and collective fraud. It benefits customers by imposing stricter penalties and establishing stronger legal mechanisms to address financial fraud targeting individuals and organizations.

3-3 The Reality of Banking Fraud in India: Banking fraud in India has shown a marked increase in recent years, as reflected in the following table:

Table (05): Trends in the Number of Banking Fraud Cases in India from 2016 to 2022

Year	2016	2017	2018	2019	2020	2021	2022
Number of Banking Fraud Cases (in thousands)	4.69	5.08	5.92	6.8	8.7	7.36	9.1

Source: Prepared by the researchers based on data from the Reserve Bank of India

The table highlights a clear increase in the number of banking fraud cases in India, rising from 4,690 incidents in 2016 to 5,080 in 2017, then to 5,920 in 2018. The upward trend continued through 2019 and 2020, reaching 6,800 and 8,700 cases respectively, before declining to 7,360 cases in 2021 amid the COVID-19 pandemic. Fraud cases rose again in 2022, reaching 9,100 incidents.

In the same context, up to 36,075 fraud cases were reported in banks during the fiscal year 2023-2024, marking an approximate 166% increase compared to 13,564 cases reported in 2022-2023.

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

According to the Reserve Bank of India's (RBI) annual report, the financial value associated with banking frauds declined by 46.7% year-on-year, falling to 13,930 crore rupees, compared to 26,127 crore rupees in the fiscal year 2022-2023.

An assessment of fraud cases by bank categories over the past three years reveals that private banks reported a higher number of fraud incidents; however, public sector banks consistently recorded the highest total monetary value of these frauds. Additionally, the majority of fraud cases occurred within the digital payments domain, particularly involving card transactions and online operations.

From a financial perspective, the RBI's annual report disclosed that 94% of the value of fraud cases reported in 2022-2023 pertained to incidents that occurred in previous fiscal years. Similarly, 89.2% of the fraud value reported in 2023-2024 was linked to events from prior fiscal years (Rimjhim, 2024).

4- Application of Artificial Intelligence in Fraud Prevention and Cybersecurity Enhancement at Punjab National Bank (PNB):

Punjab National Bank (PNB) is among India's key public sector banks and one of the oldest institutions under the supervision of the Reserve Bank of India. This section will address the status of AI implementation at PNB in combating banking fraud and strengthening cybersecurity.

4-1 Overview of Punjab National Bank: Punjab National Bank commenced operations on April 12, 1895, in Lahore, with an authorized capital of 200,000 Indian rupees and a paid-up capital of 20,000 rupees. It is an Indian multinational banking and financial services company, wholly owned by the government, headquartered in New Delhi. The bank operates more than 6,968 branches and over 9,656 ATMs across 764 cities, serving more than 80 million customers (Mohd Mustafa & Mohd, 2017, p. 06).

Key milestones in the bank's history include (Sajumon, 2025):

- 1947: Headquarters relocated to Delhi following the partition of India.
- 1969: Nationalized by the Government of India alongside 13 other major commercial banks.
- 1993: Acquired New Bank of India.
- 2002: Listed on the National Stock Exchange of India.
- 2020: Merged with Oriental Bank of Commerce and United Bank of India.
- Since 2021: Continued focus on digital banking, the Unified Payments Interface (UPI), and financial inclusion initiatives.

4-2 Use of Artificial Intelligence at Punjab National Bank (India): The AI-driven solutions implemented at Punjab National Bank include the following (By AI Storyteller, 2024):

- Enhancement of Customer Service: To offer 24/7 customer support, the bank has implemented chatbots and virtual assistants driven by AI. These systems carry out a variety of tasks, including balancing inquiries and transaction details, by using natural language processing techniques to comprehend and efficiently respond to customer inquiries.
- Detecting and preventing fraud: The bank uses AI algorithms to look at transaction patterns and find unusual ones that could be signs of fraud. Machine learning models are trained on past transaction data to find strange behavior in real time. This makes the bank's fraud prevention

strategies stronger. These predictive tools help keep the bank's money safe and build trust with customers.

- Machine learning algorithms look at more than just traditional credit scores when doing a credit risk assessment. They also look at social media activity and transaction history. With this all-encompassing approach, the bank can make better lending decisions, which means that more creditworthy clients will get their loans approved and the risk of default will go down.
- Personalized Banking Experiences: AI allows Punjab National Bank to deliver personalized banking services tailored to each customer's unique needs. By analyzing customer behavior and preferences, the bank can recommend products and services aligned with their financial goals. This personalization is achieved through advanced recommendation engines based on collaborative filtering and predictive analytics, which enhances customer engagement and loyalty.

4-3 The Reality of Banking Fraud at Punjab National Bank (India): In February 2018, Punjab National Bank experienced a significant fraud incident involving Nirav Modi and Mehul Choksi, who were implicated in a massive scandal estimated at approximately 1.77 billion US dollars at one of the bank's branches in Mumbai. This revelation severely damaged the bank's reputation; in 2017, it ranked 191st among the world's top 1000 banks according to The Banker's London ranking. The scandal sent shockwaves through the financial world (Mehrotra & Kolpula, 2024, p. 03).

This incident exemplified operational risks, stemming from bank employees deliberately exploiting flawed procedures to issue letters of undertaking for personal gain. The SWIFT system was bypassed without adequate oversight, exposing the internal banking system to fraudulent activities. Consequently, the necessity arose for standardized operational systems to ensure swift and transparent banking performance (Sudipta , 2023, pp. 60-61).

The fraud amounted to approximately 20,000 crore rupees and occurred over several years. Following the scandal, the bank's share price dropped by 10% on February 14, 2018, resulting in a loss of 4,000 crore rupees of investors' funds, equivalent to one-third of the bank's market capitalization. Investment funds holding shares in the affected bank were also impacted, as numerous mutual fund companies had invested in the bank; it was part of the equity portfolios of 117 private mutual funds.

By June 30, 2018, the gross non-performing assets (NPAs) ratio rose to 18.26% of total credit facilities, compared to 13.66% in the same quarter the previous year. Meanwhile, the net NPA ratio increased to 10.58% from 8.67% as of the second quarter of the 2017–2018 fiscal year (Salunkhe, 2018, p. 323).

Moreover, the Punjab National Bank scandal had a significant impact on the stock market. Of the 39 banks listed in India, the share prices of 34 banks declined between February 12 and February 15, 2018. These sudden price fluctuations led to a reduction in the market capitalization of these stocks by more than 36,380 crore rupees. The scandal eroded investor wealth by approximately 8,077 crore rupees. The value of fraudulent transactions at the bank was estimated to be around 50 times the bank's net profit for the third quarter of fiscal year 2018, which stood at 230.11 crore rupees (Gayathri & Mangaiyarkarasi, 2018, p. 14859).

The following table highlights the five banks directly affected by the fraudulent transactions, which had extended credit based on the letters of undertaking issued by Punjab National Bank:

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

Table (06): Banks Affected by Fraudulent Transactions Issued by PNB

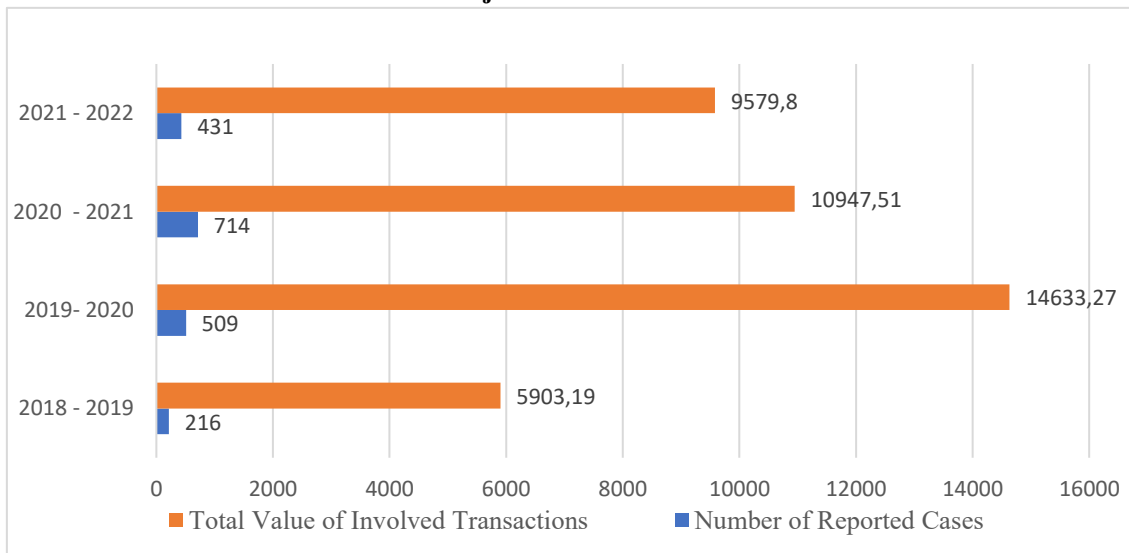
Rank	Affected Banks	Total Loss Value (Crore)	Percentage (%)
1	UCO Bank	2,635	31
2	Allahabad Bank	2,400	28
3	Indian Union Bank	1,920	23
4	State Bank of India (SBI)	1,360	16
5	Axis Bank	200	2

Source: Prepared by the researchers based on (Gayathri & Mangaiyarkarasi, 2018, p. 14859).

The table highlights that Yes Bank topped the list of banks most affected by the Punjab Bank scandal, with total losses amounting to 2,635 crore rupees, followed by Allahabad Bank with 2,400 crore rupees, and Indian Union Bank with an exposure of 1,920 crore rupees. The State Bank of India's exposure stood at 1,360 crore rupees, while Axis Bank was the least impacted with 200 crore rupees in losses.

Regarding the years following the scandal, the following figure illustrates the total number of reported fraud cases:

Figure (02): Number of Banking Fraud Cases and Total Value of Transactions Involved at Punjab National Bank



Source: Prepared by the researchers based on (Sudipta , 2023, p. 66).

The figure shows a rise in the number of reported fraud cases between 2018 and 2021, with cases increasing from 216 in the fiscal year 2018–2019 to 714 in 2020–2021. This was followed by a noticeable decline in 2021–2022, with reported cases dropping to 431. In terms of the total value involved, it rose from 5,903.19 crore rupees in 2018–2019 to 14,633.27 crore rupees in 2019–2020, before declining in the subsequent years.

To assess Punjab National Bank's efficiency in managing credit and operational risks, the development of non-performing assets (NPAs) is examined, as they serve as indicators of asset quality and financial stability. The following table illustrates the evolution of NPAs during the period 2018–2022.

Table (07): Developments in Non-Performing Assets from 2018 to 2022 (Unit: crore Indian rupees)

Statement	Mar-18	Mar-19	Mar-20	Mar-21	Mar-22
Total Non-Performing Loans (NPLs) (in million INR)	86,620.05	78,472.70	73,478.76	10,423.42	92,448.04
Net Non-Performing Loans (Net NPLs) (in million INR)	48,684.29	30,037.66	27,218.89	38,575.70	34,908.73

Source: Prepared by the researchers based on (Sudipta , 2023, p. 61).

The table illustrates the trends in gross non-performing loans (NPLs) and net NPLs, highlighting that Punjab National Bank's gross NPLs declined in the fiscal year 2019-2020 compared to 2017-2018. The gross NPLs peaked during the fiscal year 2020-2021, reaching 104,423.42 crore rupees, before decreasing again in 2021-2022. Regarding net NPLs, they were at their lowest level in 2019-2020. Based on these observations, it can be concluded that net NPLs exhibited greater stability and consistency than gross NPLs over the period from March 2018 to March 2022.

4-4 Utilization of Artificial Intelligence in Combating Banking Fraud at Punjab National Bank: Prior to implementing AI in its banking operations, Punjab National Bank assessed individuals' loan repayment capabilities manually. Currently, the bank employs AI technology for this purpose (Sabharwal, 2014, p. 03). Punjab National Bank has announced plans to apply AI in account settlement processes alongside leveraging analytics to enhance auditing systems. By deploying AI-supported auditing, the bank aims to strengthen security within its banking system by eliminating vulnerabilities, while also achieving stable growth. Key mechanisms include:

- **Activation of Integration with the National Cybercrime Reporting Portal (NCRP) via Clari5 Solution:** Punjab National Bank officially activated its integration system with the National Cybercrime Reporting Portal using the advanced technological solution provided by Clari5. This milestone represents a qualitative leap in managing cybercrime-related complaints in real time and demonstrates the bank's commitment to enhancing customer security.

This initiative supports the efforts of the Indian Cyber Crime Coordination Centre (I4C), as the new system enables immediate integration with the national portal, thereby improving fraud detection and enabling rapid, effective responses.

This solution integrates advanced automation technologies into the retail-banking environment, encompassing channels such as online and mobile banking, ATMs, debit cards, the Unified Payments Interface (UPI), and the Immediate Payment Service (IMPS). There is potential for future expansion to include credit cards and central bank digital currencies (CBDCs), in alignment with standards introduced by the I4C framework (APAC MEDIA, 2025). Key features of this technology include the following (Shukla, 2025):

-Automated Account Blocking and Freezing: The system can automatically put holds on accounts that look suspicious and freeze them when needed. This makes it easier for the bank to stop fraudulent transactions.

- Real-Time Processing Across Channels: Complaints and alerts are handled in real time across all banking channels, making sure that action is taken quickly against possible fraud.

- Customizable Whitelists : The solution lets you make your own whitelists to keep fraud prevention measures from getting in the way of real customer transactions.

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

– **Setting up a full and integrated early warning system (EWS) and smart transaction monitoring:** Punjab National Bank wants to set up a full and integrated early warning system (EWS) and smart transaction monitoring system so that they can take quick action if they think there is fraud. The bank wants to use advanced technologies like artificial intelligence, web crawling, and optical character recognition (OCR) to create dynamic early warnings based on alerts that come from borrower information gathered from a variety of internal and external sources.

By utilizing AI and machine learning techniques, this solution will be able to extract intelligent insights from diverse sources including news outlets, social media platforms, government databases, credit rating agencies, intelligence agencies, the Securities and Exchange Board of India (SEBI), the Reserve Bank of India (RBI), and other international regulatory bodies.

The system will also be capable of identifying relationships among parties connected to the borrower. Ultimately, a final score will be assigned based on the severity of indicators and the client's risk classification. By accessing a large volume of data points to assess the borrower's credibility and financial health, the program will generate real-time alerts to assist bank officials in making informed, data-driven decisions regarding the approval or rejection of transactions (India AI, 2020).

4-5 Future Prospects of Artificial Intelligence at Punjab National Bank: The outlook for AI at Punjab National Bank can be summarized as follows (By AI Storyteller, 2024):

- **Advanced Data Analytics and Big Data Integration:** The bank has the opportunity to collect and analyze massive datasets from diverse sources such as transaction histories and social media interactions. Utilizing advanced analytical techniques like deep learning and neural networks, the bank can extract profound insights into customer preferences, enabling the delivery of highly personalized services.
- **AI in Compliance and Regulatory Reporting:** AI can streamline compliance processes by automating regulatory reporting and ensuring adherence to evolving legislation. The bank can employ AI-driven systems to monitor transactions for compliance, generate reports, and detect potential violations, thereby reducing administrative burdens on staff.
- **Working together with Fintech Startups:** PNB can make strategic partnerships with AI and machine learning startups. By working with these companies, the bank can get new ideas that make it easier to do business, keep customers happy, and improve its products and services.
- **Improving Employee Training and Development:** Using AI technologies will change how things work at PNB in a big way. The bank needs to spend money on training and development programs that teach people about digital culture and AI skills so they can keep up with these changes. Giving employees the knowledge they need to use smart systems will help PNB create a culture of innovation and flexibility. This will not only make employees happier and more engaged, but it will also help the bank stay competitive in the digital age.

Conclusion:

Artificial intelligence represents a significant opportunity for banks and their customers to safeguard accounts, deposits, and funds from criminal activities. The potential applications and uses of AI are extensive; therefore, it is essential to support and further develop AI capabilities while carefully considering all associated risks and maximizing the benefits offered by the latest technologies.

This study has led to a set of findings, upon which several recommendations have been formulated:

Key Findings: The study reached the following conclusions:

- The banking sector faces numerous cybersecurity threats, including phishing attacks and data breaches.
- AI is very important for stopping fraud because it uses machine learning to find and stop fraudulent activities as they happen. This lets banks spot suspicious behavior early and look at customer patterns more closely.
- Indian banks extensively utilize AI to strengthen fraud detection systems and improve customer service.
- Punjab National Bank experienced a major fraud involving the unsupervised use of the SWIFT system, where financial transactions were conducted without adequate safeguards, oversight, or control for several years, resulting in a significant vulnerability.
- The Punjab National Bank fraud scandal exposed weaknesses in the bank's internal controls and audit mechanisms, leading to prolonged undetected fraudulent transactions. This incident negatively affected public trust in the banking sector and various Indian banks, especially amid ongoing reforms aimed at enhancing efficiency.
- In response to the scandal, Punjab National Bank adopted several mechanisms and applications to combat banking fraud and enhance cybersecurity, including the activation of integration with the National Cybercrime Reporting Portal (NCRP) via the Clari5 solution, and the implementation of a comprehensive early warning system (EWS) alongside intelligent transaction monitoring.

Study Recommendations:

Based on the findings, the following recommendations are proposed:

- It is essential to integrate banking functions with the latest artificial intelligence solutions, particularly in areas such as loan processing, high-value transactions, customer relationship management, and risk monitoring. Additionally, banks should enhance the use of AI-driven detection and response tools capable of mitigating AI-powered cybersecurity threats in real time.
- All employees should undergo regular, comprehensive cybersecurity training with an emphasis on recognizing AI-enhanced phishing attempts.
- Implement stricter identity verification and security protocols for accessing especially sensitive accounts.
- Develop effective communication strategies with institutional clients to maintain their trust even in the event of cybersecurity incidents.
- Banks should pursue partnerships with fintech companies and technology providers to enhance customer experience through AI, improve operational efficiency, and deliver automated financial services.

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

Bibliography List:

- Ballayya, S. T. (2016). Impact of Economic Reforms on Banking Sector vis A vis Liberalization. *Journal of Business and Management*, 62-66.
- Bhattacharya, C., & Sinha, M. (2022). The Role of Artificial Intelligence in Banking for Leveraging Customer Experience. *AABFJ*, 16(5), 89 -105.
- Kumar, A. S., Govardhan, D., Kaushik, W. S., Harshith, C., & Madhu, U. (2023). A CASE STUDY ON FINANCIAL FRAUD DETECTION WITH BIG DATA ANALYTICS. *International Journal of Novel Research and Development*, 8(1), 54 - 58.
- Russel, S., Perset, K., & Grobelnik, M. (2023, November 29). *Updates to the OECD's definition of an AI system explained*. Consulté le May 22, 2025, sur OECD : <https://oecd.ai/en/wonk/ai-system-definition-update>
- Salunkhe, H. (2018). Impact of PNB Scam on Banking Sector and Investors in India: An Empirical Study. *International Journal of Research in Economics and Social Sciences (IJRESS)*, 8(3), 321-326.
- Shirai, S. (2002, December). Banking Sector Reforms in India and china: Does India's experience offer lessons for china's future reform agenda? *Asia-Pacific development journal*, 9(2).
- Accenture. (2019). *Unlocking the Value of Improved Cybersecurity Protection*.
- Aksenova, M. (2024). Legal Support of Artificial Intelligence in Countering Anti-Money Laundering and Terrorism Financing Regimes in the BRICS Plus Countries. *BRICS LAW JOURNAL*, 11(3), 92- 116.
- Alrafi, H. S., & Mishra, S. (2024). The impact of AI-based cyber security on the banking and financial sectors. *Journal of Cybersecurity and Information Management (JCIM)*, 14(1), 8 - 19.
- APAC MEDIA. (2025, 01 23). *PNB Pioneers Real-Time Cybercrime Response with I4C Integration*. Retrieved May 20, 2025, from <https://apacnewsnetwork.com/2025/01/pnb-pioneers-real-time-cybercrime-response-with-i4c-integration/>
- Bukhtueva, I. (2024). HE ROLE OF AI IN FINANCIAL RISK MANAGEMENT AND FRAUD DETECTION. *International Scientific Journal Theoretical & Applied Science*, 135(07), 65 - 69.
- By AI Storyteller. (2024, 10 28). *Punjab National Bank and the Digital Revolution: Embracing AI for Enhanced Financial Services*. Retrieved MAY 19, 2025, from AI & Punjab National Bank: <https://www.cash-platform.com/punjab-national-bank-and-the-digital-revolution-embracing-ai-for-enhanced-financial-services/>
- Dawodu, O. S., Omotosho, A., Akindote, J. O., Adegbite, O. A., & Ewuga, K. S. (December 2023). CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES. *Computer Science & IT Research Journal*, 4(3), 220-243.
- Feedzai. (2024, 11 7). *Report: More Than US\$1 Trillion Lost to Scams in One Year*. Retrieved May 2025, 22, from <https://www.feedzai.com/pressrelease/report-more-than-us1-trillion-lost-to-scams-in-one-year/>
- Garifullova, D. A., & Khametshina, Z. A. (2024). Artificial Intelligence in the Banking Sector: Application Practices and Key Development Trends. *Collection of Articles from the International Scientific and Practical Conference, Petrozavodsk* (pp. 78-86). Rostov-on-Don, Russia: Science and Technologies – 2024.
- Gayathri, S., & Mangaiyarkarasi, T. (2018). A Critical Analysis of the Punjab National Bank Scam and Its Implications. *International Journal of Pure and Applied Mathematics*, 119(12), 14853-14866.

- Ghandour, A. (2021). Opportunities and Challenges of Artificial Intelligence in Banking: Systematic Literature Review. *TEM Journal*, 10(4), 1581-1587.
- Goel, S., Raut, K. D., Kumar, M., & Sharma, M. (October 2024). *How Indian Banks are Adopting Artificial Intelligence?* India: RBI Bulletin.
- Harsh, N. (2017). Critical Analysis of Banking Sector Reforms in India. *International journal on Arts Management and humanities*, 6(1), 51-53.
- HDFC BANK. (2025, Janvier 18). Retrieved May 09, 2025, from Banking Regulations and Fraud Prevention: <https://www.hdfcbank.com/personal/resources/learning-centre/vigil-aunty/understanding-banking-regulations-and-fraud-prevention-in-india>
- IBEF. (2025). *Banking Industry Report*. INDIA: Ministry of Commerce and Industry.
- IDRBT and Microsoft India. (2024). *AI in Banking: A primer*. India.
- IMF. (2024). *GLOBAL FINANCIAL STABILITY REPORT The Last Mile: Financial Vulnerabilities and Risks*. Washington.
- India AI. (2020, November 11). *AI for preventing loan frauds*. Retrieved May 20, 2025, from <https://indiaai.gov.in/case-study/ai-for-preventing-loan-frauds>
- Kamalov, M. E., & Mamatjonov, J. T. (2024, JUNE). THE ROLE OF CYBER SECURITY IN THE SYSTEM OF INTERNAL AFFAIRS BODIES AND CYBERCRIME PREVENTION. *INTERNATIONAL SCIENTIFIC JOURNAL*, 3(6), 21- 27.
- Krakowczyk, T. (2024, 09 19). *The Role of AI and Cybersecurity in the Financial Sector*. Retrieved 05 13, 2025, from SOFTWARE: <https://softwaremind.com/blog/the-role-of-ai-and-cybersecurity-in-the-financial-sector/>
- Kumar, S. (2024, 05 14). *AI-powered Fraud Detection in Banking Industry*. Retrieved May 11, 2025, from Qentelli: <https://qentelli.com/search/node?keys=+AI-powered+Fraud+Detection+in+Banking+Industry>
- Medvedeva, A., & Khvesko, T. (2021). Artificial intelligence in banking. *Международный сборник научных трудов*(10), 355-359.
- Mehrotra, S., & Kolpula, S. (2024). The Big Bank Scam: Failure of Corporate Governance. *IMIB Journal of Innovation and Management*, 2, 1- 14.
- Merriam - Webster Dictionary. (2020). *Cybersecurity*. Retrieved May 14, 2025, from <https://www.merriam-webster.com/dictionary/cybersecurity>
- Mohd Mustafa, M. S., & Mohd, T. (2017). A Study on the Financial Performance Evaluation of Punjab National Bank. *International Journal of Business and Management Invention*, 6(1), 5-15.
- Radhika, K. G. (2024). ARTIFICIAL INTELLIGENCE IN INDIAN BANKING SECTOR: AN OVERVIEW. *MSNIM Management Review*, 2(2), 1- 13.
- Rimjhim, S. (2024, 05 30). *BUSINESS STANDARD*. Retrieved May 11, 2025, from Bank frauds rise 166% in FY24 to over 36,000 cases, shows RBI annual report: https://www.business-standard.com/industry/banking/bank-frauds-rise-166-in-fy24-to-over-36-000-cases-shows-rbi-annual-report-124053001237_1.html?utm_source=chatgpt.com
- Sabharwal, M. (2014). The use of Artificial Intelligence (AI) based technological applications by Indian Banks. *International Journal of Artificial Intelligence and Agent Technology*, 2(1), 1- 5.
- Sajumon, A. (2025, 05 5). *History of Punjab National Bank (PNB)*. Retrieved MAY 19, 2025, from FYERS: <https://fyers.in/blog/history-of-punjab-national-bank-pnb/>
- Shah, C. (2024). AI Banking Paradox: InVESTIGATING Customer Awareness and Implementation in India's Financial Sector. *International Journal Of Research and Analytical Reviews (IJRAR)*, 11(3), 721-726.
- Shivani, Z., & Aditi, S. (2025, 02 5). *Artificial Intelligence (AI) in Banking Market Size, Share, and Trends 2025 to 2034*. Retrieved May 22, 2025, from Precedence RESEARCH:

The Role of Artificial Intelligence in Reducing Banking Fraud and Enhancing Cybersecurity in the Banking Sector: A Case Study of the State Bank of Punjab (India)

- https://www.precedenceresearch.com/artificial-intelligence-in-banking-market?utm_source=chatgpt.com
- Shukla, P. (2025, 01 27). *PNB Pioneers Real-Time Cybercrime Response with Clari5 Integration*. Retrieved May 20, 2025, from adda 24-7 current affairs: <https://currentaffairs.adda247.com/pnb-pioneers-real-time-cybercrime-response-with-clari5-integration/>
- Sledneva, K. E., & Kuvaldina, T. B. (2024, Сентябрь). Cybersecurity in the Financial Sector of the Economy: Necessity and Significance. *Siberian Financial School*, 3(155), 20 -27.
- Solar. (2023). *Report on Attacks Targeting the Financial Sector in 2023*. Moscow.
- Sudipta , S. (2023). Study on Artificial Intelligence (AI) in Indian Banking Sector with Special Reference to Punjab National Bank. In P. K. Paul, S. Sharma, & E. Krishnan, *Advances in Business Informatics: empowered by AI & Intelligent Systems* (pp. 48-72). India: Informatics and ICT Applications in Business series.
- VirtuBox. (2024, 09 13). *Top 11 Characteristics of Artificial Intelligence (AI) in 2024*. Retrieved May 22, 2025, from <https://www.virtubox.io/blog/characteristics-of-artificial-intelligence>
- World Bank. (2025). *Artificial Intelligence (AI) Working Group*. Retrieved May 2025, 22, from World Bank group: <https://www.worldbank.org/en/programs/govtech/artificial-intelligence>