The Chitransh Academic & Research
An International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume1 | Issue 5 | December 2025
ISSN: 3049-303X (Online)
Website: www.thechitranshacadmic.in

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN BANKING

[1]Dr.N.Malini

Assistant Professor, Department of Corporate Secretaryship, Valliammal College for Women, Chennai

[2]R.Kavitha

Assistant Professor, Department of Corporate Secretaryship, Valliammal College for Women, Chennai

ARTICLE DETAILS

Research Paper

Received: **16/12/2025**

Accepted: **21/12/2025**

Published: **31/12/2025**

Keywords: Artificial Intelligence (AI), Machine Learning (ML), Banking, Financial Services, FinTech, Credit Risk, Fraud Detection, Anti-Money Laundering (AML), Algorithmic Bias, Explainable AI (XAI), Regulatory Compliance.

ABSTRACT

Artificial Intelligence (AI) and **Machine Learning (ML)** represent the most profound technological shift currently impacting the global banking and financial services sector. This systematic review investigates the adoption, strategic impact, and critical challenges associated with the integration of AI/ML across core banking functions. We synthesize findings from scholarly and industry sources, categorizing the applications into three major domains: (1) Operational Efficiency and Automation (including document processing and cybersecurity); (2) Risk Management and Financial Crime (focusing on fraud detection, Anti-Money Laundering (AML), and credit scoring); and (3) Customer Experience and Personalization (through chatbots, robot-advisory, and hyper-personalized product recommendations). The review highlights that while AI/ML significantly enhances prediction accuracy, minimizes manual errors, and optimizes costs, its rapid deployment introduces complex ethical and legal hurdles, namely algorithmic bias, the black-box problem (lack of interpretability), and data privacy/security risks. Finally, we analyse the fragmented, yet evolving, regulatory landscape, emphasizing the imperative for financial institutions to establish robust AI governance frameworks. The paper concludes by proposing a future research agenda focused on Explainable AI (XAI) in high-stakes decisions and the development of harmonized global regulatory standards.

1 Introduction

The banking industry, characterized by vast data repositories, high transaction volumes, and stringent regulatory requirements, is undergoing a fundamental transformation driven by AI and ML. No longer confined to theoretical discussions, these technologies have moved from experimental pilot programs to mission-critical operational components. AI is not merely automating existing processes; it is enabling predictive and adaptive capabilities that redefine business models, risk assessments, and the fundamental relationship between a bank and its customers.

The pressure to adopt AI stems from a dual imperative: external competition from agile FinTech startups and internal demand for cost optimization and enhanced regulatory compliance. Traditional statistical models, based on linear assumptions, are increasingly inadequate for navigating the complexity of modern financial markets. Machine Learning algorithms, capable of non-linear analysis and continuous learning from large datasets, provide the necessary precision and dynamic adaptation.

The primary objective of this article is to systematically review the body of knowledge concerning AI/ML in banking, focusing on three key areas:

1. To delineate the key applications of AI/ML that provide tangible competitive advantage across the banking value chain.
2. To critically examine the significant technical, strategic, and ethical challenges faced during adoption.
3. To analyse the emerging global regulatory and governance frameworks essential for trustworthy AI in finance.

Literature Review

- **Conceptual Frameworks: AI, ML, and Deep Learning**

Artificial Intelligence (AI) is the overarching discipline focused on creating systems that can perform tasks typically requiring human intelligence. Machine Learning (ML) is a subset of AI

Corresponding Author: malinivcw@gmail.com

where systems learn from data, identify patterns, and make decisions with minimal human intervention. Deep Learning (DL), a subset of ML, uses layered Artificial Neural Networks (ANNs) to analyse unstructured data (e.g., text, voice, images), proving highly effective in complex tasks like speech recognition and sophisticated fraud pattern detection.

a) Risk Management and Financial Crime

This is arguably the most critical domain where AI/ML provides capabilities far exceeding traditional statistical models, transforming risk from a reactive loss-mitigation exercise into a proactive predictive capability.

- **Enhanced Credit Risk Assessment**: ML models (like Random Forests and Neural Networks) analyse vast, unstructured datasets (transaction history, web behaviour, utility payments) in addition to traditional credit scores. This allows for:
    - More Accurate Prediction: Identifying non-obvious default patterns for high-precision loan pricing.
    - Financial Inclusion: Scoring "thin-file" customers who lack traditional credit histories.
- **Real-Time Fraud Detection and Cybersecurity**: AI enables the banking system to move beyond rule-based detection, which is easily circumvented.
    - Anomaly Detection: Unsupervised ML algorithms monitor millions of transactions in real-time to spot minute deviations from a customer's normal behavior, flagging new and evolving fraud schemes instantly.
    - Adaptive Cybersecurity: AI continuously monitors network traffic and user access patterns to identify and neutralize cyber threats and insider threats autonomously.
- **Anti-Money Laundering (AML) and KYC**: AI significantly reduces the high volume of false positives generated by traditional AML systems.
    - **Intelligent Alerting:** ML models prioritize alerts based on the probability of them being genuine illicit activity, focusing human analysts on the highest-risk cases.

Corresponding Author: malinivcw@gmail.com

- **NLP for Due Diligence:** Natural Language Processing (NLP) rapidly scans news feeds, sanctions lists, and legal documents for Know Your Customer (KYC) compliance, dramatically accelerating the onboarding and due diligence process.

b) **Core Automation and Cost Reduction**

The central benefit of AI and automation is the dramatic reduction in operational costs and the acceleration of processing times by eliminating manual, repetitive work.

- **Robotic Process Automation (RPA):** RPA software "bots" are used to mimic human interactions with digital systems to execute high-volume, rule-based, and repetitive clerical tasks.
    - **Data Entry and Transfer:** Bots handle the transfer of data between disparate legacy systems and applications (e.g., inputting customer information from an application form into the core banking system), ensuring high precision and consistency.
    - **Reconciliation:** Automated systems process millions of daily transactions across different accounts and ledgers, instantly matching entries and flagging discrepancies for human review, reducing the time spent on account settlement and reconciliation from days to minutes.
- **24/7 Workflow and Scalability:** Unlike human workers, automated systems can operate around the clock with zero drop in efficiency or accuracy, providing unlimited scalability to handle peak loads or rapid business growth without major hiring sprees.

Intelligent Document Processing and Onboarding

AI, particularly Natural Language Processing (NLP) and Computer Vision (Intelligent Document Processing - IDP), is essential for automating processes that rely on unstructured data.

- **Intelligent Document Processing (IDP):** IDP technology automatically extracts, categorizes, and validates information from various document types, which are traditionally bottlenecks in banking.

Corresponding Author: malinivcw@gmail.com

- **Loan Origination:** AI reads and processes data from mortgage applications, financial statements, and supporting documents, drastically speeding up the verification and approval process.
- **KYC/AML Documentation:** NLP automatically extracts relevant entities (names, addresses, dates, affiliations) from customer identification documents and third-party news sources to perform Know Your Customer (KYC) and Anti-Money Laundering (AML) checks instantly. This accelerates customer onboarding from days to minutes.

- **Generative AI (GenAI) in Support:** GenAI is beginning to augment back-office employees by instantly summarizing complex documents, drafting audit responses, and assisting with report generation, allowing humans to focus on judgment-intensive tasks.

Regulatory and Compliance Automation (RegTech)

The regulatory burden on banks is immense and constantly evolving. AI-powered automation solutions (known as RegTech) help ensure consistent, auditable compliance.

- Automated Compliance Monitoring: AI continuously monitors transactions, internal controls, and data streams against a library of local and global regulatory rules (e.g., GDPR, Basel, AML directives).
  - It flags non-compliant activities in real-time, allowing for immediate corrective action.
- Regulatory Reporting: AI systems automatically compile, reconcile, and generate complex regulatory reports (e.g., suspicious activity reports or financial disclosure reports) from various data sources, ensuring accuracy and timely submission, which significantly mitigates the risk of fines and penalties.
- Audit Trails: Automated processes inherently create detailed, consistent audit trails for every action taken by a bot, simplifying compliance checks and external audits.

Corresponding Author: malinivcw@gmail.com

Operational Risk Reduction and Resilience

a) Reduction of Operational Risk Through Automation

Operational risk is traditionally defined as the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events. Automation addresses the "processes" and "people" components directly:

- **Minimization of Human Error:** Automated systems (RPA and AI-driven workflows) execute tasks with perfect consistency and precision, eliminating the single largest source of operational errors—human fatigue, distraction, and inconsistency in repetitive tasks. This is crucial for high-volume, sensitive processes like payment processing, account transfers, and data reconciliation.

- **Structured Control Environment:** Automated processes are governed by strict, pre-defined rules and logic. This inherent structure provides a strong, auditable control environment, ensuring that critical steps are never missed and deviations are immediately flagged.

- **Data Quality and Integrity:** AI algorithms can be implemented at data entry points to automatically validate and cleanse incoming data against established benchmarks. High-quality, consistent data is essential for regulatory compliance and accurate decision-making (e.g., credit scoring), thereby reducing the risk of decisions based on faulty input.

b) Enhancing Resilience Through Predictive Intelligence (AIOps)

Resilience refers to an organization's ability to absorb, adapt to, and rapidly recover from a disruptive event. AI significantly enhances this capability, primarily through AIOps (Artificial Intelligence for IT Operations).

- **Predictive Maintenance:** ML models analyse real-time data from the bank's extensive IT infrastructure—including network traffic, system logs, hardware health, and application performance metrics. By identifying subtle correlations and patterns that precede a failure, AI can predict system degradation or component failure (e.g., a server crash or application latency spike) hours or even days in advance.

Corresponding Author: malinivcw@gmail.com

- This allows the IT team to perform proactive maintenance or shift workloads before a service disruption occurs, ensuring continuous availability of critical banking services.

- **Intelligent Incident Response:** When an outage or security breach does occur, AI accelerates the recovery process:
  - **Root Cause Analysis (RCA):** ML quickly sifts through massive volumes of event data and alerts to pinpoint the exact source of the problem, dramatically reducing the mean time to resolution (MTTR).
  - **Automated Remediation:** For known issues, AI can trigger automated containment and remediation actions, such as isolating a compromised network segment or restarting a failing application service.
- **Security and Fraud Resilience:** AI-powered security systems learn and adapt to new threats, making them inherently more resilient than static, rule-based defences. By continuously updating threat models, the system can effectively resist evolving zero-day attacks and sophisticated financial crime tactics.

c) Business Continuity and Disaster Recovery (BCDR)

AI plays a strategic role in ensuring the bank can maintain critical functions during a crisis.

- Scenario Modelling: Advanced ML models can simulate the impact of various high-stress scenarios (e.g., a major data centre outage, a regional disaster, or a market crash) on core business functions. This helps refine and test Business Continuity and Disaster Recovery (BCDR) plans to ensure efficacy under duress.
- Dynamic Resource Allocation: In a disaster scenario, AI can dynamically re-route transaction traffic and allocate computing resources to alternative recovery sites based on real-time availability and service priorities, optimizing the minimal resources available to maintain essential services.

BCDR is typically composed of two distinct but interconnected components:[3]

Corresponding Author: malinivcw@gmail.com

- Business Continuity (BC): This focuses on maintaining critical business functions immediately *after* a disruption.[4] The goal is to keep the business running, perhaps at a reduced capacity, rather than just restoring systems. BC plans prioritize people, processes, and minimal required infrastructure.[5]
- Disaster Recovery (DR): This focuses on the technical recovery of IT infrastructure, systems, and data *after* a disaster.[6] DR plans detail the steps for restoring hardware, applications, and data backups in a designated recovery site.[7]

The Role of AI and ML in BCDR

AI and ML significantly enhance traditional BCDR by shifting the strategy from purely reactive to proactive and predictive resilience.[8]

AI/ML Enhancement	**Description**	**BCDR Impact**
Scenario Modeling& Stress Testing	Advanced ML models simulate the impact of various high-stress events (e.g., market crashes, major system outages, cyberattacks) on core business processes and financial stability.	Proactive Planning: Refines BC plans by identifying hidden vulnerabilities and testing the efficacy of recovery procedures under realistic stress, ensuring plans are viable.
Predictive System Failure (AIOps)	AI analyses system logs, performance metrics, and network traffic to predict hardware or software failure *before* it occurs.	Disruption Prevention: Allows IT teams to perform proactive maintenance, fix flaws, or migrate workloads, preventing a disruption from ever escalating into a disaster.
Dynamic Resource Allocation	During an actual crisis (like a data centre outage), AI can dynamically re-route transaction traffic and allocate	Optimized Recovery: Ensures critical services (e.g., payment processing) receive the minimal

AI/ML Enhancement	Description	BCDR Impact
	computing resources to alternative recovery sites based on real-time service health and priority.	required resources, optimizing the use of scarce recovery capacity.
Automated Incident Response	AI quickly performs root cause analysis (RCA) on system failures and, for known incident types, triggers automated containment and remediation actions (e.g., isolating an infected server).	Faster MTTR (Mean Time to Recover): Minimizes the duration of the outage, which is a key BCDR metric.

Customer Experience and Revenue Growth

AI is the engine of customer-centric banking, allowing banks to mimic the personalized, real-time engagement offered by BigTech competitors.

- **Hyper-Personalized Service and Sales:** AI analyses vast customer data to understand individual financial needs, goals, and life events.
    - Targeted Offers: Delivering the right product (e.g., a specific savings account, an investment portfolio) to the right customer at the right time, increasing cross-sell and up-sell effectiveness.
    - Proactive Advice: AI-driven financial assistants (like chatbots or virtual concierges) provide real-time budget insights and suggestions, anticipating customer needs before they are articulated.
- **Enhanced Customer Service:** Conversational AI (chatbots and voice assistants) provides 24/7, instantaneous support.

Corresponding Author: malinivcw@gmail.com

- These agents handle routine inquiries (e.g., account balance, transaction history) and often complete complex transactions, significantly reducing call centre wait times and costs.

- **Robo-Advisory and Investment Management:** ML algorithms create and manage dynamic investment portfolios.
    - By analysing market data, risk tolerance, and economic indicators in real-time, AI optimizes portfolio allocations faster and more cost-effectively than human advisors, making sophisticated wealth management accessible to a broader customer base.

Core Applications of AI and ML in Banking Operations

➢ **Revolutionizing Credit Risk Management**

Traditional credit scoring models (e.g., logistic regression) rely on a limited set of structured data (credit history, income). ML models, such as **Random Forests** and **Artificial Neural Networks**, fundamentally reshape this process by:

- **Integrating Alternative Data:**Analysing vast, unstructured data (e.g., social media activity, utility payments, browser history, transaction patterns) to assess creditworthiness for "thin-file" or previously unscoreable populations, thus promoting financial inclusion.
- **Dynamic Default Prediction:** Continuously learning and dynamically adjusting a customer's probability of default based on real-time behaviour and macroeconomic variables, significantly outperforming static, historical models.
- **Risk-Based Pricing:** Enabling highly granular risk segmentation, allowing banks to offer personalized interest rates and terms, optimizing profitability and reducing loss exposure.

➢ **Combating Financial Crime: Fraud and AML**

Financial institutions must monitor billions of transactions globally, making traditional rule-based fraud detection obsolete. AI provides a critical defence layer:

Corresponding Author: malinivcw@gmail.com

- **Real-Time Anomaly Detection:** ML algorithms (especially unsupervised learning models) are adept at identifying subtle deviations from established transactional or behavioural norms (anomalies) in real-time, which are indicative of new, evolving fraud schemes.

- **Enhanced AML/KYC:Natural Language Processing (NLP)** and **Generative AI (GenAI)** are used to rapidly process vast quantities of unstructured data (news articles, sanctions lists, legal documents) to streamline KYC checks and flag suspicious activity faster and with greater precision than human analysts, improving regulatory compliance and reducing false positives.

Content Snippet 1 (Cybersecurity): AI's role in cybersecurity is shifting from reactive detection to **predictive and adaptive defence**. ML models monitor network traffic and user behaviour patterns to identify, isolate, and respond to cyberattacks and insider threats autonomously, often before they can cause material damage. This includes the use of **federated learning** to share threat intelligence across financial institutions while preserving data privacy.

➢ **Customer Experience and Service Automation**

AI has become the face of modern digital banking, improving both efficiency and customer satisfaction:

- **Intelligent Chatbots and Virtual Assistants:** Powered by GenAI and sophisticated NLP, these tools handle complex customer queries, account maintenance, and even product sales (e.g., loan pre-qualification), offering 24/7 service and dramatically lowering contact centre costs.

- **Hyper-Personalization:** ML algorithms analyze customer journeys, peer interactions, and financial goals to deliver **hyper-personalized recommendations** for banking products (e.g., customized savings accounts, investment advice), increasing product uptake and customer loyalty.

Corresponding Author: malinivcw@gmail.com

The Challenges of AI Implementation: Ethics, Transparency, and Governance

Ethical Challenges: Bias and Fairness

The most pressing ethical challenge is the risk of **algorithmic bias**, which can lead to unfair or discriminatory outcomes.

- **Bias in Training Data:** AI models are trained on historical data, which often reflects and embeds past human and systemic biases (e.g., historical lending discrimination based on race or gender). When the AI system learns from this flawed data, it perpetuates and *scales* these biases into new, automated decisions like credit scoring, loan approvals, or even fraud flagging.

- **Proxy Discrimination:** Even if a bank excludes sensitive demographic data (like race or gender) from the model, the algorithm can still identify and rely on **proxy variables** (e.g., ZIP code, certain spending patterns) that correlate strongly with protected characteristics, leading to *de facto* discrimination.

- **Socio-Economic Impact:** The widespread use of biased AI in high-stakes decisions risks **exacerbating financial exclusion** by unfairly denying services to certain demographic groups, contradicting a bank's commitment to fairness and often violating anti-discrimination laws (like the Equal Credit Opportunity Act in the US).

Transparency Challenges: The "Black Box" Dilemma

The inherent complexity of powerful ML and Deep Learning models creates a problem of **opacity**, known as the "black box" dilemma.

- **Lack of Interpretability:** In many complex ML models, even the creators cannot precisely explain *how* the algorithm arrived at a specific decision. It provides an output (e.g., "deny loan") but not a clear, human-readable justification.

- **Regulatory Conflict (Right to Explanation):** This opacity directly conflicts with regulatory and consumer rights that require financial institutions to provide a **"Right to Explanation"** for adverse decisions (e.g., why a loan was denied or an account frozen).

Corresponding Author: malinivcw@gmail.com

Without transparency, banks cannot comply with these mandates, exposing them to significant legal and reputational risk.

- **Model Auditing Difficulty:** The lack of transparency makes it extremely difficult for regulators, internal auditors, and risk management teams to **validate, audit, and stress-test** the model to ensure it is working as intended, not introducing bias, and remaining stable under different economic conditions.
    - **Solution Focus: Explainable AI (XAI):** The industry is pushing for **XAI** techniques (like LIME and SHAP) to make model decisions interpretable without sacrificing prediction accuracy.

Governance and Accountability Challenges

Implementing AI requires new governance structures to manage ethical dilemmas, assign responsibility, and ensure continuous oversight.

- **Accountability and Liability:** When an AI system makes an erroneous or harmful decision (e.g., an automated trading system causes a loss, or an AML model falsely flags a legitimate customer), it is often unclear **who is legally accountable**—the data provider, the model developer, the deploying business unit, or the Chief AI Officer. Existing legal frameworks struggle to assign liability to an autonomous system.
- **Data Privacy and Security:** AI systems thrive on vast amounts of data, often containing sensitive **Personally Identifiable Information (PII)**. This necessitates **robust data governance** frameworks to ensure compliance with global data protection laws (like GDPR), manage data lineage, and prevent misuse or breaches, which are magnified by the sheer volume of data involved.
- **Model Risk Management (MRM):** Traditional MRM frameworks must be updated to handle unique AI-specific risks, such as **model drift** (where accuracy degrades over time as real-world data changes) and the potential for **adversarial attacks** (where an attacker subtly manipulates input data to trick the AI). This requires **continuous, real-time monitoring** of AI models post-deployment.

Corresponding Author: malinivcw@gmail.com

- **Regulatory Uncertainty:** The AI regulatory landscape is still fragmented and evolving (e.g., the EU AI Act, various central bank guidelines). Financial institutions must adopt a **risk-based approach**, applying the strictest governance to **high-risk applications** like credit scoring, while adapting agilely to new legislation.

Conclusion

AI and ML have proven to be indispensable tools for the modern banking sector, driving unprecedented gains in efficiency, security, and customer personalization. The transformative potential is undeniable, particularly in areas like real-time fraud detection and next-generation credit risk modelling.

However, the path forward is contingent upon addressing the profound ethical and governance challenges. The successful bank of the future will be defined not just by the sophistication of its algorithms, but by its ability to demonstrate trustworthiness, fairness, and transparency in their deployment. The "black box" cannot remain a defence against scrutiny.

Future Research Agenda

1. **Long-Term Socio-Economic Impact:** Quantitative studies on the long-term effects of AI-driven hyper-automation on the financial labour market and wealth distribution.
2. **XAI and Regulatory Compliance:** Comparative analysis of XAI techniques (LIME, SHAP) on their effectiveness in meeting evolving global regulatory standards for transparency in high-stakes financial decisions.
3. **Adversarial AI and Defence:** Research into the development of robust, resilient ML models capable of detecting and neutralizing sophisticated **adversarial attacks** (e.g., data poisoning) in real-time.

References

- Louzada, F., Faria, V. F., & Junior, G. E. D. (2020). Credit scoring: A comparison of machine learning models. *Expert Systems with Applications*, 148, 113261.

Corresponding Author: malinivcw@gmail.com

- Bahnsen, C., Stojanovic, N., & Pedersen, M. A. (2017). Machine learning for credit card fraud detection—Practical approaches. *IEEE Intelligent Systems*, 32(6), 49-55.
- Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Luque, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges. *Information Fusion*, 58, 136-157.
- Bank for International Settlements (BIS). (2021). *The regulatory implications of BigTechs' entry into fin*

Corresponding Author: malinivcw@gmail.com