IJAFIBS, 13 (1) (2025) pp. 86-95

Published by: TRIGIN Publisher

International Journal of Applied Finance and Business Studies

Journal homepage: www.ijafibs.pelnus.ac.id

Overcoming the challenges of ai adoption in banking sector: Security, regulation, and infrastructure

Novi Handayani Simbolon[1], Fatma Dwi Jati[2], Sondang Beatrix Siahaan[3]

[1,2]Jurusan Akuntansi, Politeknik Negeri Medan, Indonesia

[3]Jurusan Administrasi Niaga, Politeknik Negeri Medan, Indonesia

ARTICLE INFO

Article history:

Received Jun 5, 2025
Revised Jun 7, 2025
Accepted Jun 11, 2025

Keywords:

Artificial Intelligence;
Cybersecurity;
Fraud Detection;
Regulatory Compliance;
Risk Assesment.

ABSTRACT

The adoption of Artificial Intelligence (AI) in the banking sector has rapidly expanded, because bringing benefits in areas such as risk assesment, fraud detection, and personalized services. However, AI adoption faces significant challenges related to security, regulation, and infrastructure. While previous research has explored AI's potential, there is a gap in comprehensive studies addresing these core challenges, particularly in emerging markets. This research aims to identify and analyze the main barriers to AI adoption in banking, focusing on security, regulatory issues, and infraastructure readiness. A systematic literature review was conducted, synthesizing findings from academic articles, banking reports, and regulatory guidelines published between 2020 and 2024. The result reveal that concerns over data security, inconsistent regulations, and insuffiecient infrastructure hinder AI's full potential. The concludes of this research showed banks must prioritize cybersecurity, advocate for clearer regulations, and invest in digital infrastrcuture to ensure the secure AI adoption in banking activities.

Corresponding Author:

Novi Handayani Simbolon,
Program Studi Keuangan dan Perbankan,
Politeknik Negeri Medan,
Jalan Almamater No.1, Medan 20155, Indonsesia
Email: novihandayani@polmed.ac.id

1. INTRODUCTION

The development of Artificial Intelligence (AI) has brought about a profound transformation across various sectors, including banking, by unlocking new possibilities for innovation and operational efficiency. AI, as a disruptive technology, has become an essential tool for banks seeking to stay competitive in an increasingly digital and data-driven landscape. It offers a wide range of benefits, such as enhancing operational efficiency, accelerating service delivery, improving decision-making, and strengthening financial security. In particular, AI applications in banking have revolutionized areas such as risk assessment, fraud detection, credit scoring, and customer service automation. Furthermore, AI has enabled personalized banking services that cater to the unique preferences and needs of individual customers, offering them more tailored and efficient solutions (Department of the Treasury, 2024).

Operational complexity in the banking sector serves as both a driver and a barrier to the integration of Artificial Intelligence, particularly in the domains of security, regulation, and infrastructure. On one hand, this complexity acts as a significant barrier due to the widespread use of legacy systems, fragmented data architecture, and siloed operations, which make it difficult to deploy AI solutions seamlessly. These outdated systems often lack the interoperability and processing capabilities required for AI, raising security concerns and implementation costs.

Furthermore, strict regulatory requirements, such as those related to anti money laundering (AML), data protection and financial transparency impose additional constraints, as AI models must be auditable, explainable, and compliant with legal standards across multiple jurisdictions. Risk-averse organizational cultures within banks, shaped by a need to avoid disruption and maintain trust, further complicate adoption. On the other hand, the very nature of this operational complexity also acts as a catalyst for AI integration. The scale and intricacy of banking processes, such as fraud detection, compliance reporting, and customer service create strong demand for automation and intelligent decision-making. AI is increasingly being adopted to enhance operational efficiency, reduce errors, and provide real-time insights that traditional systems cannot offer. Moreover, as cyber threats grow more advanced, AI becomes essential in safeguarding banking infrastructure through predictive threat detection and automated responses. Regulatory complexity, too, has spurred innovation in regulatory technology (RegTech), where AI is used to automate compliance tasks and adapt to evolving legal frameworks. Thus, while operational complexity introduces substantial challenges, it simultaneously highlights the necessity of AI, positioning it not merely as a tool for innovation, but as a critical enabler for managing the demands of a modern, secure and compliant banking environment.

The level of AI adoption in the banking sector significantly differs between emerging and developed economies, both quantitatively and qualitatively. In developed economies, banks typically invest their annual IT budgets on AI related initiatives, backed by mature digital infrastructure, regulatory support, and availability of skilled talent. In contrast, banks in emerging economies allocate significantly lower AI spending often below 2% due to budget constraints, limited digital infrastructure, and a shortage of AI professionals. Furthermore, while developed markets are advancing toward explainable AI and regulatory aligned AI ethics, emerging economies are still addressing basic digitization gaps, such as migrating from paper-based processes to digital platforms. However, mobile first markets are showing promising progress in AI driven financial inclusion through chatbots, credit scoring for the unbanked, and fraud monitoring in mobile banking. These contrasts reveal a clear digital and AI maturity gap, though the rapid mobile penetration and fintech growth in emerging markets offer unique leapfrogging opportunities if adequately supported by infrastructure and regulation.

Despite its growing adoption and transformative potential, the implementation of AI in banking is not without its challenges. One of the most pressing issues faced by financial institutions is the aspect of security (Ochell Andrea & Yudha Febrianta, 2024). The integration of AI systems into banking operations introduces new vulnerabilities, particularly in terms of data breaches and cyberattacks. As financial services become more digitized and interconnected, the risk of cyber threats increases significantly, leaving sensitive customer data exposed to malicious actors. AI systems, while capable of enhancing security protocols, also create new opportunities for cybercriminals to exploit weaknesses in the system. For this reason, banks must invest heavily in cybersecurity measures to protect their digital infrastructure, safeguard customer data, and maintain trust in their services. Implementing robust cybersecurity frameworks is not merely a technical necessity but also a critical step in ensuring the long-term viability of AI adoption in banking.

(Listyono Putro et al., n.d.) In addition to security concerns, regulatory challenges also present a major barrier to the widespread adoption of AI in the banking sector. The legal and regulatory frameworks governing the use of AI in financial services remain underdeveloped in many regions, particularly in emerging markets (Lukita Nova Azzara & M. Ruslianor Maika, 2025). Regulatory uncertainty surrounding AI technologies creates a complex environment for banks, which must navigate conflicting or ambiguous policies on data protection, algorithmic decision-making, and accountability for AI-driven actions. For example, the use of AI for automated decision-making, such as credit scoring or loan approvals, raises concerns about fairness, transparency, and the potential for algorithmic bias. Without clear and consistent regulations, financial institutions face the risk of non-compliance, legal challenges, and damage to their reputation (Niroula & Adhikari, 2024). Policymakers must therefore address these gaps by developing comprehensive regulatory frameworks that provide clear guidance on the responsible use of AI in banking while ensuring consumer protection and data privacy.

The third significant challenge that banks face when adopting AI is infrastructure readiness. AI technologies require advanced digital infrastructure, including access to vast amounts of data , powerful computing capabilities such as cloud computing, and skilled human resources with expertise in AI and data analytics (Ramadhani & Trimuliani, 2024). Banks, especially those in developing economies, often struggle with outdated or legacy IT systems that are incompatible with modern AI technologies. These legacy systems, which were designed for traditional banking operations, are not equipped to handle the scale and complexity of AI-driven processes. Moreover, the implementation of AI requires substantial investments in upgrading digital infrastructure, as well as ongoing training and development of human capital to support these new technologies. Without the proper technological foundation, the adoption of AI in banking will face significant hurdles, slowing down the digital transformation process and limiting the full potential of AI applications.

(Lazo & Ebardo, 2023) In light of these challenges, this research aims to explore the key barriers to AI adoption in the banking sector, with a particular focus on security, regulatory, and infrastructure-related issues. (Padilla Hernández, 2024) By conducting a systematic review of the literature, the study seeks to identify the main obstacles to AI implementation and to offer strategic recommendations for overcoming these challenges. It is anticipated that the findings will provide valuable insights not only for academics and researchers but also for banking industry practitioners and policymakers (Tong & Yang, 2025). Understanding the complexities surrounding AI adoption in banking will enable institutions to develop more effective strategies for integrating AI technologies, addressing security and regulatory concerns, and investing in the necessary infrastructure. Ultimately, this research aims to contribute to a deeper understanding of how AI can be responsibly and securely integrated into banking operations, fostering a more resilient, efficient, and customer-centric banking ecosystem.

(Ikhsan et al., 2025) Security remains one of the most pressing challenges faced by banks as they incorporate advanced technologies into their operations. With the increasing use of sophisticated systems in banking, the associated risks related to cyber threats have also grown. While these technologies offer substantial benefits, such as improving fraud detection and automating customer service, they also create new vulnerabilities that can be exploited. For example, some systems can be vulnerable to manipulation, where malicious actors may intentionally alter data to deceive these processes, leading to incorrect conclusions or even allowing unauthorized access to sensitive information. This raises significant concerns regarding the protection of personal and financial data. As these systems process larger volumes of sensitive information, the risk of breaches or misuse becomes more pronounced, potentially leading to significant financial and reputational damage.

(Soelistyo Budi et al., n.d.) To address these risks, banks must invest heavily in enhancing their security measures. This includes adopting advanced encryption techniques, implementing multi-factor authentication, and continuously updating security protocols to protect customer data. Additionally, a proactive approach is needed to monitor systems for potential vulnerabilities, using regular security audits, testing for weaknesses, and improving data protection practices (Judijanto & Yuniarti, 2024). A crucial aspect of this strategy is fostering a culture of security awareness across the bank, ensuring that all staff understand the risks and the measures required to mitigate them effectively.

(Maseke, 2024) The regulatory environment surrounding the adoption of advanced technologies in the banking sector is still evolving. While these innovations hold immense potential to transform banking operations streamlining processes, automating complex tasks, and enhancing decision making the absence of clear, comprehensive regulations presents a significant challenge. In many regions, legal frameworks that govern the use of such technologies remain underdeveloped, particularly when it comes to issues like privacy, accountability, and the transparency of automated decision-making systems. For example, when banks utilize advanced systems for tasks such as credit scoring, loan approval, or risk assessments, it raises critical questions about the fairness and transparency of these decisions (Farishy, 2023). Without established guidelines on how these systems should function, banks are exposed to the risk of facing regulatory scrutiny or even legal action. Moreover, concerns about data privacy are at the forefront, as these technologies often rely on vast amounts of personal information to process

decisions. If not carefully managed, the collection and use of such sensitive data could compromise customer privacy and trust.

To address these regulatory challenges, it is essential for banks to engage in proactive dialogue with policymakers and regulators. By working together, it will help shape regulations that are not only clear and enforceable but also flexible enough to adapt as technologies continue to evolve. (Rustandi & Arifin, 2024) Establishing transparency in decision-making processes, such as providing customers with insight into how their data is being used, will be key to building and maintaining trust in these technologies. Furthermore, ongoing international discussions aimed at developing global standards for the use of advanced technologies in banking are crucial. These efforts will ensure that technological advancements are aligned with regulatory frameworks, preventing the emergence of legal ambiguities that could hinder the growth and adoption of these innovations (Byambaa et al., 2025).

(Abdulsalam & Tajudeen, 2024) Artificial Intelligence (AI) is reshaping the global banking landscape, offering new capabilities in areas such as customer personalization, fraud detection, credit risk analysis, and process automation. However, while the potential benefits of AI are well-recognized, its successful implementation hinges on more than just algorithms and data scientist, it requires a fundamental transformation of the underlying infrastructure. In many traditional banking institutions, legacy IT systems, fragmented data silos, and outdated architectures pose substantial barriers to AI integration. These legacy systems were designed for reliability and compliance in a different era, not for the speed, flexibility, and computational intensity that modern AI technologies demand (Nadzirin Anshari Nur & Kassymova, 2025).

AI systems thrive on large volumes of high-quality, real-time data, robust computing power, and scalable, flexible platforms. Yet many banks struggle with basic infrastructural limitations, such as poor data interoperability, limited cloud adoption, and rigid monolithic system designs. These limitations not only slow down AI deployment but also increase operational costs and security risks. Additionally, the lack of agile infrastructure impedes banks from experimenting with AI innovations and adapting quickly to market changes or regulatory demands (Geetha, 2021).

(Preeti Arora, 2023) Modernizing infrastructure is thus a strategic priority for banks seeking to harness AI effectively. This involves embracing cloud computing, implementing data integration platforms, building secure and scalable data pipelines, and adopting modular, API driven architectures. Furthermore, institutions must cultivate a technology environment that supports continuous learning, experimentation, and collaboration between IT, data science, and business units. Without this foundational shift, even the most advanced AI models will fail to deliver their intended value (Shaikh et al., 2024).

2. RESEARCH METHOD

This research conducted a systematic literature review approach to examine the key challenges in adopting Artificial Intelligence (AI) within the banking sector, with a specific focus on issues related to security, regulation, and infrastructure. The systematic literature review method was chosen to ensure a comprehensive and structured synthesis of existing academic and industry knowledge on the topic. Data were collected from a wide range of sources, including peer reviewed academic journals, industry reports, regulatory publications, and conference proceedings published between 2020 and 2024. These sources were retrieved from reputable databases Google Scholar as well as official documents issued by financial regulatory authorities, including Bank Indonesia and Otoritas Jasa Keuangan (OJK). The inclusion criteria for selected literature were, firstly, the study was published between 2020 and 2024. Secondly, the focus was on the application or challenges of AI in the banking or financial sector. Thirdly, the article discussed at least one of the core topics security, regulation, or infrastructure. Fourthly, the full text of the publication was accessible. After collecting the relevant studies, the researcher conducted a thematic analysis to identify and categorize recurring themes and findings. The analysis was structured around three main dimensions: security, regulatory framework, and infrastructure readiness. Within each dimension, the review explored specific challenges faced by banking institutions in implementing AI technologies, especially in the context of emerging markets. Furthermore, the analysis considered differences across geographic regions, highlighting contextual factors that influence AI adoption in

various regulatory and technological environments. To ensure the reliability and validity of the findings, the study employed data triangulation by comparing insights from academic literature with real-world case studies, regulatory guidelines, and industry practices. This triangulated approach helped to bridge the gap between theoretical perspectives and practical realities, providing a more holistic understanding of the barriers to AI adoption in the banking sector and offering recommendations for overcoming them.

The systematic literature review method is a structured approach that helps address potential publication bias and the underrepresentation of local contexts, particularly from emerging markets, by implementing a transparent, reproducible, and inclusive search strategy. Unlike traditional narrative reviews, this method define explicit inclusion and exclusion criteria, allowing researchers to systematically scan a broad range of sources including peer-reviewed journals, conference proceedings, gray literature, and regional databases to capture diverse perspectives beyond high-impact Western publications. By expanding the scope to include local case studies, policy reports, and non English publications, this method can uncover insights from underrepresented regions that are often overlooked in mainstream literature. Moreover, through the use of quality appraisal tools, systematic literature review assess the methodological rigor of each source, helping to balance the influence of heavily cited but potentially biased studies. To further mitigate bias, researchers can adopt bibliometric techniques and citation tracking to identify less visible but contextually rich contributions from local institutions or regional regulatory.

3. RESULTS AND DISCUSSIONS

The results of this research that the adoption of Artificial Intelligence (AI) in the banking sector is hindered by three critical and interrelated challenges, that are security vulnerabilities, regulatory ambiguity, and infrastructure limitations. These barriers are especially prevalent in emerging markets, where digital transformation in the financial industry is still at a nascent stage. While AI promises significant advantages in improving operational efficiency, enhancing customer service, and reducing fraud, these benefits are contingent upon addressing the underlying issues that obstruct AI's full scale deployment. The following discussion explores each of these challenges in detail and their implications for banking institutions. Several countries have established regulatory sandboxes and cross sector initiatives to facilitate responsible AI adoption in the financial sector by allowing innovation under controlled environments. One notable example is the UK Financial Conduct Authority (FCA) Regulatory Sandbox, which has enabled fintech firms to test AI based solutions, such as automated financial advice and fraud detection tools while being closely monitored by regulators. This framework has not only reduced the time to market for emerging technologies but has also helped build regulatory trust. Similarly, Singapore's Monetary Authority (MAS) operates a robust sandbox program and has launched the Veritas initiative, which promotes the responsible use of AI and data analytics in finance by offering an open source framework for fairness, ethics, accountability, and transparency. These initiatives exemplify how regulatory flexibility, combined with collaboration between policymakers, academia, and the private sector, can accelerate AI deployment while safeguarding consumer protection and financial stability. An effective AI governance model in banking must be multi-dimensional, integrating technical robustness, legal compliance, and organizational alignment to ensure trustworthy AI adoption. Technically, the model includes principles such as data quality assurance, algorithmic transparency, and continuous model monitoring to prevent biases, errors, or security vulnerabilities. Legally, it embeds compliance frameworks that align with international regulations such as Basel III and local data protection laws, ensuring that AI systems are explainable and accountable particularly critical in high stakes decisions like loan approvals or fraud detection. On the organizational level, the model promotes cross functional AI committees that include representatives from compliance, IT, operations, and ethics departments, thereby fostering a culture of shared responsibility. It also introduces standard operating procedures (SOPs) for AI deployment, incident response, and third-party AI vendor risk management. By holistically addressing these three pillars, the governance model ensures that AI systems are not only technically sound but also legally defendable and institutionally integrated, reducing the risk of regulatory breaches, reputational damage, or ethical lapses.

The causal relationship between weak infrastructure and vulnerable security systems is both conceptually logical and practically observable, particularly in developing financial ecosystems. Conceptually, infrastructure forms the foundational layer upon which digital and security systems are built. When infrastructure is weak characterized by outdated hardware, unreliable network connectivity, low data processing capacity, and insufficient redundancy, it creates gaps and inefficiencies that make it difficult to implement or sustain modern cybersecurity frameworks. Practically, these limitations expose banks to increased risks of breaches, service outages, and unauthorized access. For instance, without robust data centers, encrypted communication channels, and real-time monitoring capabilities, financial institutions are unable to deploy AI based intrusion detection systems or maintain secure, compliant data storage. Moreover, inadequate infrastructure often leads to dependency on legacy systems, which are known to be more susceptible to known vulnerabilities and lack support for modern encryption standards or multi-factor authentication. In such environments, even the best designed AI security models cannot operate effectively due to constraints in computational power, integration capabilities, or system interoperability. This dependency forms a vicious cycle, where poor infrastructure limits the adoption of secure technologies, and in turn, weak security erodes trust in digital banking, discouraging further investment in infrastructure. Thus, improving infrastructure is not just a technical necessity but a strategic imperative for enhancing the resilience and trustworthiness of AI enabled banking systems.

Security Vulnerabilities in AI Driven Banking Systems

One of the most cited concerns in the reviewed literature is data and system security. AI applications in banking rely heavily on vast datasets, often containing highly sensitive personal, financial, and behavioral information. This dependency raises significant risks around data privacy, model security, and system integrity. The literature revealed that many AI-driven solutions, especially those involving machine learning and predictive analytics, are susceptible to adversarial attacks situations where attackers manipulate input data to deceive the AI models into making incorrect predictions. For example, fraud detection algorithms may be misled through spoofed transactions, leading to false negatives that allow fraudulent activities to go unnoticed. Additionally, most conventional cybersecurity frameworks used by banks are not fully equipped to handle AI specific threats. These systems often lack capabilities such as real-time threat detection for AI pipelines, secure model deployment environments, or automated patching for AI vulnerabilities. Furthermore, as banks adopt third party AI tools, often via APIs or Software as a Service (SaaS) models, the risk of supply chain attacks increases. In such cases, the bank's data may be exposed not through direct hacking but via a breach in a less secure third-party provider.

Compounding these issues is the lack of customer trust in AI-based decision-making, particularly in regions where awareness about data rights and cybersecurity is growing. Consumers are increasingly concerned about how their data is used and the ability of banks to safeguard that information against misuse. In light of this, banks must not only implement robust technical safeguards such as end-to-end encryption, multi-layered access control, and anomaly detection but also work on building transparent communication channels to educate customers and regulators about their AI security practices.

Regulatory Ambiguity and Lack of Standardization

Another key barrier to AI adoption in banking is the absence of clear and harmonized regulatory frameworks. The research uncovered that many banking institutions face uncertainty regarding compliance obligations when deploying AI systems, particularly in relation to data protection, automated decision-making, and explainability. This regulatory uncertainty is especially problematic in emerging economies, where legislative structures are still adapting to the digital age. Unlike regions with established data protection laws, many countries lack specific policies governing how AI systems should operate within critical sectors like finance.

This regulatory gap has led to a fragmented landscape, where some banks take a conservative approach delaying AI adoption until clearer guidelines are provided while others proceed at risk, hoping to adapt retroactively if required. A specific concern raised in several studies is algorithmic bias, especially in AI models used for credit scoring or customer profiling.

Without regulatory mandates for fairness and accountability, such systems may unintentionally discriminate based on race, gender, geography, or socioeconomic status. This not only exposes banks to reputational and legal risks but also conflicts with their social responsibility commitments.

Moreover, regulators themselves are often under-equipped to evaluate AI systems. There is a lack of technical expertise in many supervisory bodies, and few institutions have developed the capability to audit AI algorithms effectively. The lack of explainability the ability to interpret and justify AI decisions further complicates compliance efforts. Most deep learning models operate as black boxes, making it difficult for banks to explain why a loan was denied or why a particular transaction was flagged as fraudulent. Consequently, there is an urgent need for regulatory sandboxes and cross sector collaborations that allow banks to experiment with AI under monitored conditions while contributing to the development of appropriate legal standards.

Infrastructure Limitations and Technological Gaps

The third major challenge is the infrastructure gap faced by many banking institutions, especially in developing regions. Effective AI deployment requires not only software tools but also a foundational technological ecosystem that supports real-time data processing, scalable computing resources, and reliable connectivity. Many banks still rely on legacy IT systems that are siloed, inflexible, and incompatible with modern AI tools. These outdated systems often lack the ability to handle large-scale data analytics, limiting the bank's capacity to train and deploy intelligent models.

One significant limitation is the absence of centralized data lakes or unified data architectures, which are essential for effective AI training and inference. Many banks store their data in fragmented systems, making data integration a major hurdle. This fragmentation not only slows down AI development but also leads to inconsistent results, poor performance, and increased operational risk. Furthermore, while cloud computing offers a solution to scalability and processing power, adoption is limited due to concerns about data sovereignty, latency, and regulatory compliance. Some institutions are hesitant to move sensitive financial data to the cloud due to fears about cross-border data flow and potential breaches in shared environments.

The human capital aspect is also noteworthy. The study identified a shortage of skilled AI professionals in many banking organizations. This includes data scientists, machine learning engineers, and AI ethicists who are crucial for the safe and effective deployment of AI systems. In some cases, even when the bank is ready to invest in AI, the lack of internal expertise and over-reliance on external vendors leads to superficial adoption with limited strategic value. To overcome these limitations, banks must undertake a phased modernization of their IT infrastructure, integrating hybrid cloud systems, adopting API-based architectures, and investing in staff training programs to upskill existing employees. Public private partnerships may also play a role in improving technological readiness by facilitating knowledge sharing and capacity building initiatives.

Interdependencies and Strategic Implications

Importantly, these three challenges security, regulation, and infrastructure are not isolated but rather highly interconnected. Weak infrastructure undermines the implementation of strong security measures. Inadequate regulatory guidance leads to hesitancy in investing in new systems. Poor cybersecurity practices hinder both regulatory compliance and infrastructure trustworthiness. Therefore, an effective response requires a holistic, strategic approach that addresses all three areas in parallel. Banks are encouraged to develop a comprehensive AI governance framework that encompasses risk assessment, legal compliance, technical auditing, and continuous monitoring. Security should not be treated as a separate domain but integrated throughout the AI lifecycle from data collection and preprocessing to model training, deployment, and post-decision auditing. Regulators, in turn, should evolve toward adaptive regulation, allowing for dynamic oversight mechanisms that accommodate fast evolving AI technologies. Industry bodies and policymakers must also collaborate to create interoperable regulatory standards and provide technical support to under resourced institutions.

4. CONCLUSION

This study has explored the multifaceted challenges impeding the adoption of Artificial Intelligence (AI) in the banking sector, with a particular focus on three core areas, such as security, regulation, and infrastructure. The results, derived from a systematic literature review of recent studies, reveal that although AI holds tremendous potential for transforming banking operations enhancing efficiency, improving risk management, and personalizing customer service its adoption is significantly constrained by vulnerabilities and gaps within these foundational domains. Security remains a pressing concern, as banks grapple with the responsibility of protecting vast volumes of sensitive data used by AI systems. The threat of adversarial attacks, data breaches, and unregulated third-party access highlights the need for banks to build AI-specific cybersecurity frameworks. These must go beyond traditional IT security approaches and include robust mechanisms for securing data pipelines, ensuring model integrity, and protecting customer privacy.

To foster responsible and effective AI adoption in the financial sector, regulators in developing countries must craft legal frameworks that are both progressive and sensitive to local institutional, technological, and socio economic realities. First, regulators should establish AI regulatory sandboxes tailored to local market maturity, enabling financial institutions and fintech innovators to test AI applications, such as credit scoring or fraud prevention in a controlled environment while engaging regulators early in the development cycle. Second, it is essential to adopt a principle-based rather than prescriptive regulatory approach, focusing on core values like fairness, accountability, and transparency, while allowing flexibility for future technological developments. Third, regulators should promote inter-agency and cross-sector collaboration bringing together financial authorities, data protection agencies, technology experts, and consumer advocacy groups to ensure that legal frameworks reflect diverse perspectives and evolving risks. Fourth, local regulations must prioritize data governance and digital infrastructure readiness, including provisions for secure data sharing, local data sovereignty, and interoperability standards. Finally, capacity building is crucial, regulators should invest in training programs and institutional expertise to better understand AI systems, assess algorithmic risks, and respond to compliance challenges. By combining global best practices with localized insight, regulators can create enabling environments that support innovation, strengthen financial inclusion, and safeguard public trust in AI driven banking.

Regulatory uncertainty further complicates AI adoption. Many banking institutions operate in legal environments where there is little or no guidance on how AI should be deployed, monitored, or held accountable. This lack of clarity discourages innovation and heightens institutional risk, especially when it comes to explainability and fairness in automated decision-making. Regulatory bodies, in turn, must accelerate the development of coherent and technology-aware policies that balance innovation with consumer protection, data sovereignty, and ethical responsibility. Infrastructure challenges also play a crucial role, particularly in emerging markets where digital maturity is still evolving. Legacy systems, fragmented data environments, and limited access to scalable computing resources severely hinder the development and deployment of AI solutions. Furthermore, the shortage of skilled professionals capable of designing, implementing, and maintaining AI technologies within banking institutions exacerbates these limitations.

The success of safe and responsible AI adoption in the banking sector can be assessed through a combination of short-term operational indicators and long-term strategic outcomes, each aligned with principles of security, compliance, efficiency, and trust. In the short term, measurable indicators include a reduction in fraud incidents through AI-based detection systems, improvements in response time for customer service via AI chatbots, and compliance rates with internal AI governance protocols, such as model validation, fairness audits, or explainability standards. Additionally, uptime and stability of AI-driven platforms, incident response speed, and user satisfaction scores can signal early-stage success. In the long term, success is reflected in more systemic and sustainable outcomes such as regulatory acceptance and certification of AI systems, increased financial inclusion through AI powered credit scoring for underserved populations, and strengthened cyber resilience demonstrated by consistent defense against evolving threats. Moreover, the presence of a mature AI governance framework, sustained investment in AI related talent and infrastructure, and public trust in AI assisted banking services are strong indicators of long term success. Banks that can demonstrate transparency, accountability, and equitable access

through their AI systems over time are more likely to gain competitive advantage while fulfilling ethical and regulatory expectations. Tracking these indicators holistically allows institutions to balance innovation with responsibility in their AI transformation journeys.

The interplay between these challenges underscores the need for an integrated strategy. Addressing one barrier in isolation is insufficient. Banks must simultaneously invest in digital infrastructure, strengthen cybersecurity practices, and engage proactively with regulators to build a trusted and transparent AI ecosystem. Collaboration across financial institutions, technology providers, and regulators is essential to ensure the responsible and sustainable implementation of AI in the banking sector. Overcoming the challenges of AI adoption in banking is not merely a technological endeavor, it is a strategic transformation that requires commitment to secure systems, clear regulations, and scalable infrastructure. Only by confronting these challenges holistically can banks unlock the full potential of AI to innovate, compete, and serve customers in a digital future.

REFERENCES

Abdulsalam, T. A., & Tajudeen, R. B. (2024). Artificial Intelligence (Ai) In The Banking Industry: A Review Of Service Areas And Customer Service Journeys In Emerging Economies. Business & Management Compass, 68(3), 19–43. Https://Doi.Org/10.56065/9hfvrq20

Byambaa, O., Yondon, C., Rentsen, E., Darkhijav, B., & Rahman, M. (2025). An Empirical Examination Of The Adoption Of Artificial Intelligence In Banking Services: The Case Of Mongolia. Future Business Journal, 11(1), 76. Https://Doi.Org/10.1186/S43093-025-00504-Y

Department Of The Treasury, U. (2024). Managing Artificial Intelligence-Specific Cybersecurity Risks In The Financial Services Sector.

Farishy, R. (2023). Attribution-Sharealike 4.0 International (Cc By-Sa 4.0) The Use Of Artificial Intelligence In Banking Industry. Www.Statista.Com

Geetha, A. (2021). A Study On Artificial Intelligence (Ai) In Banking And Financial Services. Www.Ijcrt.Org

Ikhsan, R. B., Fernando, Y., Prabowo, H., Yuniarty, Gui, A., & Kuncoro, E. A. (2025). An Empirical Study On The Use Of Artificial Intelligence In The Banking Sector Of Indonesia By Extending The Tam Model And The Moderating Effect Of Perceived Trust. Digital Business, 5(1). Https://Doi.Org/10.1016/J.Digbus.2024.100103

Judijanto, L., & Yuniarti, D. (2024). Artificial Intelligence In Banking: The Future Of Digital Financial Services. International Journal Of Financial Economics (Ijefe), 1(1), 119–128.

Lazo, M. P., & Ebardo, R. A. (2023). Artificial Intelligence Adoption In The Banking Industry: Current State And Future Prospects. Journal Of Innovation Management, 11(3), 54–74. Https://Doi.Org/10.24840/218

Listyono Putro, R., Rapini, T., Farida, U., Budi Utomo No, J., Ponorogo, K., & Timur, J. (N.D.). Analisis Penerapan Kecerdasan Buatan (Artificial Intelligence) Untuk Meningkatkan Keamanan Finansial Nasabah Pada Sektor Perbankan Universitas Muhammadiyah Ponorogo, Indonesia. Https://Doi.Org/10.61132/Lokawati.V3i1.1433

Lukita Nova Azzara, & M. Ruslianor Maika. (2025). Applications Artificial Intelligence (Ai) And Machine Learning (Ml) In The Mobile Banking Services Industry: A Bibliometric Review. Ekspektra : Jurnal Bisnis Dan Manajemen, 9(1), 33–46. Https://Doi.Org/10.25139/Ekt.V9i1.9527

Maseke, B. F. (2024). The Transformative Power Of Artificial Intelligence In Banking Client Service. South Asian Journal Of Social Studies And Economics, 21(3), 93–105. Https://Doi.Org/10.9734/Sajsse/2024/V21i3787

Preeti Arora. (2023). Msw Management-Multidisciplinary, Scientific Work And Management Journal. Msw Management, 33(2), 444450. Https://Mswmanagementj.Com/

Nadzirin Anshari Nur, M., & Kassymova, G. K. (2025). The Potential Misuse Of Artificial Intelligence Technology Systems In Banking Fraud. In Universitas Diponegoro (Vol. 21, Issue 1).

Niroula, A., & Adhikari, S. (2024). Machine Learning, Banking, Industry, Digitalization, Innovation. American Journal Of Finance And Business Management, 3(1), 62–72. Https://Doi.Org/10.58425/Ajfbm.V3i1.286

Ochell Andrea, N., & Yudha Febrianta, M. (2024). Pengaruh Artificial Intelligence Terhadap Acceptance Of Ai Enabled Banking : Studi Kasus Pada Livin' By Mandiri. 8(3).

Padilla Hernández, S. G. (2024). Artificial Intelligence In Banking Services. A Bibliometric Review. Región Científica. Https://Doi.Org/10.58763/Rc2024335

Ramadhani, F., & Trimuliani, D. (2024). Pemanfaatan Sistem Artificial Intelligence Pada Industri Perbankan: Systematic Literature Review. Jurnal Mutiara Akuntansi, 9(1), 37–49. Https://Doi.Org/10.51544/Jma.V9i1.5281

Rustandi, R., & Arifin, A. H. (2024). Ai In Finance: A Systematic Literature Review (Vol. 1, Issue 2). Https://Prosiding.Areai.Or.Id/Index.Php/Iceat

Shaikh, A. A., Kumar, A., Mishra, A., & Elahi, Y. A. (2024). A Study Of Customer Satisfaction In Using Banking Services Through Artificial Intelligence (Ai) In India. Public Administration And Policy, 27(2), 167–181. Https://Doi.Org/10.1108/Pap-05-2023-0060

Soelistyo Budi, H., Sudirman, L., & Afdal, W. (N.D.). Analisis Risiko Finansial Perbankan Melalui Artificial Intelligence (Ai): Politik Hukum Dan Potensi Pengembangan Hukum. Https://Doi.Org/10.24843/Jmhu.2025.V14.I01

Tong, X., & Yang, W. (2025). Empirical Analysis Of The Impact Of Financial Technology On The Profitability Of Listed Banks. International Review Of Economics And Finance, 98. Https://Doi.Org/10.1016/J.Iref.2024.103788