Regulatory compliance with AI and risks involved in finance and banking sectors

Reshma Sudra

Email id: Sudra.Reshma@gmail.com

Abstract Artificial intelligence is an essential part of the world and acts as a powerful catalyst driving transformative modifications in various industries. AI encompasses different technologies such as computer vision, language processing, and machine learning. The financial sector has integrated AI technology into services and products. The introduction of artificial intelligence in banking services has transformed the sector into more customer-oriented and technologically relatable. Regulatory compliance is considered armor since it protects financial institutions from vulnerabilities that can lead to irrecoverable damages and hefty fines. The current study examines regulatory compliance with AI and the risk involved in the financial and banking sectors. AI in banking and other financial institutions enhances the customer experience, security, and efficiency. AI positively influences the banking sector and offers many advantages. The present study analyses the regulatory compliance with AI and threats in banking sectors involving AI. The main risks are security threats such as data breaches, adversarial attacks, and lack of transparency. Furthermore, the current study investigates the challenges in regulatory compliance with AI and deploying AI in the financial sector. The widespread integration of technologies such as AI in the financial sector has some major concerns. Banks also encounter various challenges, such as data privacy and data security, in leveraging technologies related to AI. The banking industry requires strong security measures to prevent violations and breaches. Therefore, the study also recommends integrating firmer privacy policies, regulatory framework, and technical solutions to balance AI's advantages and protect customer's privacy.

Introduction

A. Theoretical Background

In past decades, the world has undergone many changes, especially during the occurrence of a new wave of technologies extended among various industries. Through utilizing technologies, many industries have improved their performance and capabilities. The introduction of technologies to any industry comes with multiple complexities and challenges across technical, social, adoption, and regulatory-related areas. There is a need for power to operate, maintain, and design the system inside the constellations of an organization. However, trust is considered to be related to the technology and performers who govern the technology (Janssen, Weerakkody, Ismagilova, Sivarajah, & Irani, 2020). Many service-oriented industries, from telecom and manufacturing to banking, are interested in the benefits of the new digital technology as these have enabled new business simulations. All service industries at present are either testing or using digital technologies to transform the business method. A wide range of technologies like the Internet of Things (IoT), 3D printing, cloud computing (CC), and artificial intelligence (AI), along with blockchain has the main scope in the industries. The benefits of these technologies are security, predictive ability during dynamic conditions, and self-learning capacity. Digitalization, new technologies, and innovation transform traditional business processes and models (Kitsios, Giatsidis, & Kamariotou, 2021).

Developments and sustainable information technology (IT) changes have been widely adopted in the banking business (Mbaidin, Alsmairat, & Al-Adaileh, 2023). In the financial sector, security is an important concern, and technologies implemented in the banking and financial service sector play a vital role such as CC helps to integrate the data and requirements of customers with knowledge acquired to offer personalized facilities in the

banking sector, IoT employed to payments, insurance and banking activities, Machine learning (ML), a kind of AI technology support banks to offer customer quick service and comply with rules and regulations. Additionally, technologies are frequently used for regulatory purposes. Financial institutions (FI) and banks are meant to be the lifeline of current society and perform as stimulators in nourishing and improving the economic development of developing countries. The banking industry is challenged with fraudulent transactions, increasing operational prices, and transparency. Because the system must ensure transparency for regulators and customers and guarantee cost-efficient operations. The banking sector must investigate and execute robust technologies to prevent and process transactions quickly. In addition, banks have adopted many different platforms driven by technologies to improve banking activity functions (Garg et al., 2021). To address this challenge, two primary approaches can be considered:
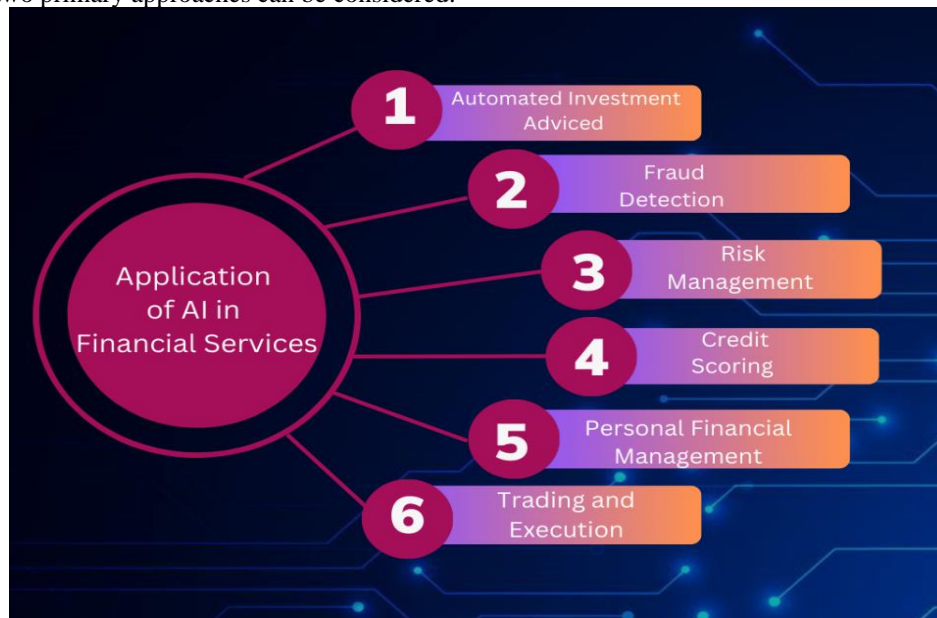

Figure 1 Application of AI in the banking and financial sector (Rohada, 2023)

In the period of the modern banking system, many new technologies are AI-driven and act as a strategic engine leading to innovative changes in banking services, solutions, and channels. AI empowers the banking sector to completely change the system's functions and demonstrate innovative services and products. For the purpose of maintaining a competitive edge, the financial and banking sectors embrace AI in their market strategy (Yanting & Ali, 2023). The main objective of all the businesses is to reduce the risks involved in the business, including financial and banking institutions. Since banks deal with payments and deposits, fraudulent activities are considered a serious challenge, and AI technologies help prevent such activities with predicting ability. AI is considered a topmost technology that comes with fraud detection methods and security. It also examines a person's previous spending behavior and pattern toward the different transactions and finds the odd behaviors immediately. AI has the potential to learn things based on experience and act accordingly in times of crisis (Malali & Gopalakrishnan, 2020).

Algorithm-driven technologies such as AI are rapidly pervading all aspects of human life (Smuha, 2021). AI technologies bring new challenges and complexities, demanding banks to understand and abide by the relevant regulations. These risks comprise data breaches, job displacement, cyber security threats, and biased judgments. Examining such risks can discover possible vulnerabilities and execute suitable risk mitigation tactics, which help to protect sensitive data and act against discriminatory outcomes. In addition, this proactively reports the influence of AI on the personnel. Hence, the present research study emphasizes the role of AI in the bank and financial sector, the risks involved, and the regulatory compliance of AI

B. Significance of the study

The banking sector is under a radical shift; the emergence of non-bank companies is altering the competitive landscape in fiscal service, and AI is very promising in the banking sector (Königstorfer & Thalmann, 2020). Regulatory compliance and risk management (RM) are necessary for maintaining an optimistic reputation and forming trust with investors, regulatory bodies, and customers. With the appropriate implementation of AI technologies, expert knowledge, and a great understanding of regulatory compliance needs, updating banking compliance (BC) becomes a planned initiative that reduces risks, improves operational efficiency, and strengthens the bank's entire regulatory position. The present study examines the regulatory compliance with AI

and risks involved in the finance and banking sector as AI technology constantly advances, and it is important to comply with and understand the regulations that govern AI uses. Compliance guarantees that AI systems are deployed and developed in such a manner that aligns with ethical and legal standards, protecting consumers and businesses. The problems involved in the banking and finance sectors with AI are multifaceted. Understanding regulatory compliance with AI and challenges in the finance and banking sector can enhance the advantage of AI when mitigating possible pitfalls, ensuring secure and responsible implementation. Thus, the current study examines regulatory compliance with AI and the risks involved in the banking and finance sector.

C.   Problem Identification

The finance and banking sectors are largely regulated to guarantee fair practices, stability maintenance, and protect consumers of the banking system. The banking sectors handle the the customer's personal, financial, and sensitive information. AI systems that process all such data should be implemented and designed with caution to protect user privacy and against misuse and leakage of data. Some businesses face challenges to ensure that AI systems follow ethical and legal standards which could even lead to reputational damage and potential penalties when failed. Banking is a highly regulated industry of the economy worldwide. Banks use regulatory authorities to avoid risk profiles, which have the potential to cause large-scale non-payments and ensure no customers use banks to commit financial crimes. Regulatory compliance has been a most important challenge of the banking industry as it directly impacts the dramatic rise in regulatory price relative to credit losses and earnings. All these challenges can be resolved by implementing AI to monitor, audit, and follow up on customer behavior. Hence, the present study is essential to analyze the significance of AI regulatory compliance and risks in the finance and banking sectors.

D.   Objectives of the research study

The present study emphasizes regulatory compliance with AI and the risks involved in the finance and banking sectors. The research objectives of the current study are,

[1]. To overview the influence of AI in investment sectors and its beneficiaries.
[2]. To discuss the regulatory compliance with AI and risks involved in the finance and banking sectors.
[3]. To study challenges of banking regulatory compliance and difficulties involved in deploying AI in the financial sector.
[4]. To recommend future strategies to overcome the challenges effectively.

E.   Paper Organisation

The paper is organized in the following order Section 1 provides an elaborated introduction regarding the regulatory compliance with AI and the risks involved in the finance and banking sector. Furthermore, the introduction section illustrates the significance of the research. In section 2, prevailing research works related to the current study will be reviewed. The current study's section will elucidate the role of AI in the banking and finance sector with challenges. In section 4, the outcome of the current research will be discussed. In section 5, the analysis outcome will be discussed with existing studies. Finally, in section 6, the brief conclusion regarding the current study will be discussed along with future recommendations.

Literature Review

The existing study (Rahman, Ming, Baigh, & Sarker, 2023) determined to analyze the challenges and importance of adopting AI in the banking sector in Malaysia. In addition, it examined the components which are significant in exploring consumer's perception of the adoption of AI in financial services. The prevailing study applied mixed research methodology, consisting of qualitative and quantitative methods. The qualitative approach collected data from banking authorities using interview instruments, and quantitative data was gathered from 302 customers of Malaysian banks through a questionnaire. The accumulated data were analyzed using SmartPLS software to discover the significant factors. The prevailing study resulted in AI being necessary for risk prevention and fraud detection. The significant challenges for AI implementation are data privacy, IT infrastructure, regulatory requirements absence, and skills. The factors influencing the intention of implementing AI in financial services were a risk, trust, and perceived usefulness. The study concludes that the mediating factor between the intention to use AI in banks and perceived usefulness was the attitude directed towards AI.

The existing study (Mohsen, Hamdan, & Shoaib, 2024) determined to investigate the impact of adopting AI on financial services, customer experience, and products. In addition, it explored various aspects of A1, including process automation (PAM), chatbots (CB), predictive analysis (PA), and ML. The prevailing study adopted a mixed research methodology, applying both qualitative and quantitative methods for analysis purposes, including secondary data exploration, and the analysis was carried out for AI subfields. The study showed that implementing AI, especially in chatbots and ML subfields, provides high tactical potential for FI, which enhances customer experience and services. Furthermore, the importance of PA integration and PAM was found

to be comparatively low. The study concludes that AI implementation reduces human errors and interaction in FI.

The existing study (Carmody, Shringarpure, & Van de Venter, 2021) demonstrated privacy concerns increasing from the quickly rising developments and use of AI technology and the difficulties of already present privacy systems to guarantee the ongoing safety of a person's sensitive personal information. The prevailing study illustrated using a smart meter attained energy data case study. The case study demonstrated how data related to energy consumption could be combined with different data to obtain sensitive data such as household income, lifestyles, and other personal information. The exploration resulted in data privacy and protection concerns not being discovered immediately due to advancements in AI. Consumers' private information can be exposed to energy data such as frequency, usage time, and household appliance details. The study concludes that AI has the potential to extract personal and sensitive information when employed on large, overlying granular datasets and proves the risk of data privacy in the adoption of AI.

The existing study (Kumar & Suthar, 2024) determined to investigate the AI's legal and ethical distress in marketing and feasible solutions for concerns. The prevailing study collected secondary data from case studies, academic articles, and legal documents using a thematic review and industry reports. A qualitative research approach was employed to categorize and find legal and ethical challenges present with the intention of proposing feasible solutions for respective concerns. The analysis resulted in significant ethical concerns regarding bias, job displacement, environmental impact, and cyber security. The Legal and privacy concerns such as responsibility, competition law, consumer protection, consumer security, liability, and brand protection are discovered as main challenges in the marketing field, along with possible solutions such as transparency, establishing ethical rules, and implementation of appropriate tools to secure the privacy of consumers. The study concludes that adopting an innovative and appropriate framework reduces the AI complexities in marketing, and a comprehensive attitude is essential in addressing ethical and legal concerns.

The existing study (Mogaji & Nguyen, 2022) purpose was to investigate the awareness among managers regarding AI and the complexities in offering assistant technologies. In addition, the study emphasized the main stakeholder cooperative efforts in delivering financial services. The prevailing study applied an exploratory research design and collected data using semi-structured interviews with 47 managers of banks in both developing and developed countries such as the UK, Nigeria, Vietnam, and Canada. The results indicated that bank managers are aware of the AI aspect and proposing methods to integrate AI as a business requirement, a conceptual framework was proposed to emphasize communication among regulators, banks, and customers. In addition, the managers are challenged in accelerating the adoption of AI in the banking system.

The existing study (Lupo, 2023) focused on AI incidents and an efficient tactic of data gathering and analysis to enhance knowledge of the influence of AI technologies and standardize them better. Applied mixed research methodology, which includes both quantitative and qualitative analysis techniques. The prevailing study results indicated the significance of generating effective tactics for analyzing AI influence in various contexts and supported effective AI laws. Incident analysis of different sectors may provide AI regulation in sectors where AI has not been significantly diffused, like the justice sector. The study concludes that AI's main challenge and risk were different interest contexts of applications.

A. Research Gap

[1]. The existing study (Kumar & Suthar, 2024) has not discussed other effects, such as concerns related to intellectual property, licensing, and contracts. The prevailing study is limited to the marketing industry and secondary data analysis.

[2]. The existing study (Mogaji & Nguyen, 2022) has not explored the significance of ethical implications and comprehending the requirement of customers in financial services to implement AI and use it efficiently.

AI In the Finance and Banking Sector

A. Evolution of banking compliance

Compliance is an important element of the banking sector which ensures the institutional operations within the limits of regulatory laws. The outcome of failing to obey this guideline is severe, ranging from huge fines to irreparable reputation damage to an institution. Hence, it is necessary to execute comprehensive compliance procedures and policies. BC is a set of policies, laws, and policies that FI must follow to guarantee that their activities are ethical, secure, and legal. This prevents money laundering and illegal practices such as fraudulent activities.

Compliance with norms, regulations, and laws helps every bank maintain its reputation, enabling it to meet the demands of society, the market, and customers. Banks that are negligent in performing the role and purpose of compliance face compliance risk, which is generally known as material loss, damage to the bank's reputation, and legal risks as a consequence of violating and not following regulations, rules, and laws related to norms. In

the banking and financial sector, reputation is essential because it guarantees uninterrupted performance development. Compliance risk emerges when banks fail to implement or comply with applicable regulations and laws. As a result, compliance with RM is necessary to avoid the risk of increasing and distributing funds along with other service-related activities, which can increase creditability and public trust (Hobvi, Zunaidi, & Fikriyah, 2022).

Compliance with corporate governance (CG) with effective regulations is essential for the banking sector to accomplish legitimacy in the community. In addition, executing applicable corporate governance is essential for maintaining and cultivating public confidence (Zulfikar et al., 2020). Moreover, the ineffective execution of CG leads to a crisis in banking. As a consequence, a main effect of unsuccessful bank governance is reducing trust among the public about banks, which indirectly affects the economy. This is due to bank managers increasing bank failure and reducing the chances of economic development and corporate finance. In the age of globalization, Banks must take advantage of other external ideas and development outcomes along with regulations from outside the bank, which is generally known as open innovation. The banking company's innovations regularly obey the regulations from external circles, specifically regulators, and the execution of CG.

Compliance with CG practices is inevitable in modern-day business management, which is entirely supported by money and capital markets since it has the potential to improve trust among the public. Non-compliance with CG in the banking sector leads to scandals and financial crises because of poor supervision. CG compliance plays a significant part in industry sustainability. Compliance with CG in the banking sector is a way to prevent the public from losses in bank investment.

Over the years, BC has experienced a noteworthy evolution. From being seen as a legitimate activity to becoming an essential component of RM, compliance has been considered an important factor in FI. The evolution of BC is driven by different factors, comprising developments in technology, modifications in frameworks related to regulations, and the demand to handle emerging risks. Some aspects include increased regulatory analysis, embracing technology, data security, data privacy, RM, collaboration, and more. The following are some key features:

Regulatory Scrutiny: Regulatory forms strengthened their management of the banking sector to guarantee financial stability and prevent customers from any losses. This has resulted in the beginning of firmer enforcement measures and new regulations. As governments in all countries worldwide have announced new guidelines and regulations to prevent financial crimes, FI had to adapt rapidly to stay and remain compliant. This eventually resulted in a transformation directed to more practical compliance strategies, and many institutions invested in technologies and compliance technologies.

Proactive RM: Compliance operations have transformed from a reactive tactic to a more practical proactive RM management method. Banks focus on finding and mitigating compliance risks in advance so the risks don't escalate, with the help of risk assessments, frequent monitoring, and scenario analysis. With the great threat of cybercrime and the increase in technologies, FI faces new risks that require sophisticated RM strategies.

Embracing technology: Banking industry transformation in digital has a significant influence on compliance. Banks and FI have adopted advanced and improved technologies such as ML, automation, and AI to improve their compliance process. All technologies support banks in detecting and preventing financial crimes, enhancing RM, and streamlining compliance functions.

The introduction of digitization and automation has modernized compliance activities. Manual works such as data entry, report generation, and document management are now automated, which reduces human mistakes and enhances efficiency. This enables compliance professionals to concentrate on more strategic and complex tasks. The use of AI revolutionized risk assessment and compliance monitoring. AL algorithms analyze a large amount of data, and detect irregularities and patterns along with possible compliance breaches. This allows the identification of damages and intervention at the right time, which improves the effectiveness of efforts in compliance. Digital biometric authentication, data analysis, and identity verification allow more efficient and precise customer meticulousness, decreasing the risk of fraud and theft related to identity. Technology has enabled the execution of a robust KYC (Know your customer) process. KYC regulations have become rapidly severe in the fight against terrorist financing, money laundering, and other illegal activities (Parate, Josyula, & Reddi, 2023). Banks have executed robust systems and processes to monitor transactions, report suspicious functions, and verify consumer identities. Banks have prioritized data security and privacy nowadays. Compliance efforts include measures to prevent leakage of customer information and follow data protection rules, as well as implement cyber security protocols. Overall, the involvement of technology in BC improved accuracy, RM capabilities, and efficiency.

B. Banking compliance department and its role

The BC is an essential component of FI's operations. Its main role is to guarantee that the FI complies with all relevant regulations and laws, thus preventing data theft. The demand for a devoted compliance department

(CD) has increased as FI has developed in complexity and size. The banking CD establishes and implements procedures and policies that promote compliance with regulations, industry standards, and laws. The primary role of bank CD is to implement BC, policy and manage residual risks (RR). Especially to emphasize the implementation and transparency of BC.

To implement BC, establishing a clear compliance policy (CP) is vital with all relatable regulations and legislation. Standardization and management are considered an essential process for a successful bank CDs. Executing standards for finding risks, improving resolution, problem management, and making inventories. The banking CP is an important document that outlines the management's structure for compliance with regulations, industry standards, and laws. After executing control to avoid risks, it is necessary to examine the RR. For managing RR, there are four categories: mitigation, acceptance, avoidance, and transfer.

Figure 2 Bank Compliance (Watson, 2021)

The bank CD uses AI technology to improve its functions and guarantee adherence to supervisory demands. AI technology is applied to analyze a large amount of data and detect anomalies and patterns in transactions. This supports the department in supervising and avoiding money laundering, fraudulent activities, and compliance breaches. The algorithm of AI can assist in automating processes related to compliance, such as regulatory reporting, enhancing accuracy and efficiency. The incorporation of AI in CD aims to reinforce regulatory compliance and maintain the reliability of the FI. The bank CD leverages AI in various ways to improve its operations and guarantee regulatory compliance. There are a few particular ways AI is utilized such as:

KYC: AI-based systems help in automating the customer due diligence and KYC processes. AI screen customer against sanction lists and watch list and examine the risk related with customers. AI also helps in reorganizing the onboarding process when ensuring compliance with counter-terrorism financing and anti-money laundering regulations.

Regulatory reporting (RR): AI automates the submission and generation of RR like suspicious transaction and activity reports. By extracting relatable data from different sources and applying rules, the AI system ensures precise reporting at the right time, which reduces the burden of compliance officers.

Fraud Detection: AI detects anomalies and patterns in transactional data, customer behavior, and customer account activities to find possible fraud cases. Through constantly extracting historical data, AI improves bank's fraud detection abilities and acclimates to progressing fraud methods.

Risk Assessment: AI models analyze different data sources, comprising social media, market trends, and news articles, to examine the entire risk coverage of the FI and banks. This supports CD in finding possible risks, validating the effectiveness of already present controls, and judgments made using data to avoid possible compliance risks.

AI significantly improves the effectiveness and efficiency of bank CD; human management and expertise stay important in interpreting AI insights, making judgements, and guaranteeing responsible and ethical utilization of AI technology in the Bank.

C.   A lack of transparency

The main challenge in implementing AI is the accomplishment of quality assurance regardless of the crucial demand for coherence and transparency. AI results, including calculations, processes, decisions, and projections. Although the intention of an AI is programmed, the process for achieving it is trained. So, the process and product in the AI elements act inversely. This renders some risks, such as data bias. Appropriate control tools are needed for supervising the AI's behaviour, which makes it difficult to integrate into the industry along with

its adherence to standards and regulations. The technological challenges in AI adoption are that it requires a large amount of data to generate processes, the lack of transparency in the market, and the unavailability of technology providers hinder the integration of AI in banking services. The deprived transparency of the system AI black box leads to doubts. Ultimately, the banking sector finds it difficult to adopt AI because of transparency and reliability factors (Thowfeek, Samsudeen, & Sanjeetha, 2020).

AI lack transparency in various ways. The main reason is the complexity of AI models and algorithms. This lack of transparency is commonly known as "black box" issue. Dependency on datasets for AI model training is a major reason for transparency issues, as datasets contain inaccurate and biased data, which can influence the result of AI and lead to discriminatory and unfair outcomes. In addition, the proprietary AI system nature which were developed for organizations. Management generally keeps models and algorithms confidential for security and competitive advantage reasons, making it challenging for external factors to examine the internal working and validate possible biases and ethical considerations. Concerns about the ability and accountability to reason out the decisions made using AI, especially in critical processes of banking such as fraud detection and loan approvals, are raised with AI models (Yu & Song, 2021).

Transparency in banking using AI is very important for creating trust among customers and banks. By promoting transparency in FI and banks, they can offer customers the needed information to decide and understand the importance of AI system action and recommendation. This allows for responsibility and the ability to identify possible issues and biases from the AI algorithm. AI banking's lack of transparency defines the challenges in understanding how AI is utilized in the banking sector, especially in decision-making related to financial services and transactions. Technologies of AI are frequently being applied in banking to improve efficiency, customer experiences and tasks. However, the lack of transparency arises because bank users are unaware of how AI algorithms implemented in banks are used to finalize direct decisions that impact their lives, meaning the financial aspect (Ashta & Herrmann, 2021).

Trust and transparency are complex in AI banking and trust is a key component for the success of AI integration. Especially, when AI is involved in financial decisions. Financial decisions are considered as high-stakes activities, and customers can even lose money in such decisions. Customers in banking services, unlike customers in other automatic systems, are inclined to be vulnerable. Any untrustworthy and unfair perception will negatively affect the adoption of AI among customers. Customer's understanding of data offered through AI is also necessary. Lack of human assistance and experts or explanations, customers depend on their understanding while using AI, which has more visualized data. The black box algorithm in the system makes it difficult for customers to understand the reason for the decision made. This leads to low adoption and distrust in AI decisions (Zhu, Pysander, & Söderberg, 2023).

Data issues	Trust issues	Economical issues	Technical issues
• Availabilty of data • Reliabilty of data • Data ownership	• Human-machine interactions • Robots stealing jobs • Mistrust in higher-ups and their decisions • Misuse of technology	• Capital cost • Less jobs • Scarcity of skilled workforce • Legislations • Funding requiremnets and sources	• System reliability • Application at large scale • System security and data breach • Malwares, viruses, and cyber attacks • Troubleshooting

Figure 3 AI challenges (Hyder, Siau, & Nah, 2019)

The AI system's nature is dynamic, which makes it challenging to track and brief their process of decision making. AI-based models constantly learn and adapt to new data, making offering a static and clear explanation for actions challenging. Industry organizations and regulatory bodies are working to establish standards and guidelines for transparency in banking. The purpose is to guarantee customers have access to understandable and clear information on ways AI is utilized, including the features considered in making decisions, the data utilized, and the possible limitations and biases of the AI.

D. Data security and privacy

The widespread integration of AI technologies raises significant risk, security, and trust concerns. Risks include unintended outcomes, biases, ethical concerns, and data privacy (Habbal, Ali, & Abuzaraida, 2024). Organizations have privacy and security concerns resulting in an unwillingness to integrate AI systems. Securing the privacy of users and AI systems creates trustworthy systems. However, AI systems are exposed to

various privacy risks, such as the data gathering phase, which may be present in data storage. The inability to differentiate nonsensitive data from sensitive data during modeling and pre-processing phases endangers data privacy. It is legally must for government offices and other organizations to secure and protect all sensitive and personal data. There exists a complicated phenomenon related to application and privacy of data where there is no way to increase privacy without losing application data (Alzubaidi et al., 2023).

AI models and systems are designed without consideration for privacy and security, which makes them vulnerable to adversarial. These attacks occur during the testing or training phase of ML. Adopting AI systems in various applications offers a unique way to solve many environmental and socio-economic challenges. However, without concentrating on methods to secure these technologies (Oseni et al., 2021). AI brings various advantages to the banking sector, but it has security threats related to privacy and security that need immediate attention. There are some security concerns related to AI in FI and banking such as:

Data breaches: AI models and systems often rely on large amounts of data, including sensitive information such as personal details. If not appropriately secured, sensitive data can be exposed to breaches leading to potential misuse and unauthorized access.

Privacy concerns: AI models process and examine a large amount of data, increasing threats to privacy. If the case is not properly protected or anonymized, a person's privacy rights might be violated. Data anonymization is a common way to protect data privacy. However, AI technology development raises re-identification risks where protected data is linked to individuals. This poses a security and privacy threat along with confidentiality.

Data sharing: AI often depends on the data from different sources comprising third-party data providers. The data sharing among various entities increases concerns about how data is maintained, protected, and stored, possibly compromising privacy.

Bias: AI systems and algorithms can unintentionally prolong biases in the trained data. This leads to discriminatory results, such as decisions made with partialities and unfair treatment of particular groups or individuals.

Adversarial attacks: This kind of attack involves intentional manipulation and misleading AI systems by introducing malicious feedback. Adversarial attacks exploit AI algorithms vulnerabilities which leads to biased and incorrect outcomes.

These data security and privacy threats need a comprehensive tactic that includes strong data protection methods, encryption techniques, regular security checks, recent AI system evaluation and supervision, and implementing technologies for enhancing data privacy. Addressing the issues also demands the integration of technical resolutions, regulatory frameworks, and privacy policies. It is important to prioritize data privacy and security to ensure ethical and responsible AI deployment and development (Elliott & Soifer, 2022).

Discussion

The present study represents regulatory compliance with AI and risks involved in the finance and banking sector. The significance of AI in the investment field and its beneficiaries are highlighted. The current study also emphasizes the challenges in the banking system related to regulatory compliance and implementing AI. Overall, the study demonstrates the significance of AI regulations and the complexities involved.

The existing study (Chadha, Gera, Khera, & Sharma, 2024) illustrates the challenges in implementing AI in the fiscal inclusion of the omitted and applied unobtrusive research method. The result of the conventional study listed challenges involved in AI adoption, such as deployment risk, cyber-attacks, and data protection. Similarly, the current study identifies the main challenges in deploying AI in the financial sector. In addition, the outcome of the present study demonstrates the AI risks involved in the banking and financial sectors along with complications.

The existing study (Hu & Wu, 2023) demonstrates the significance of regulatory compliance and the risks involved with non-compliance. The outcome of the prevailing study highlights the significance of constantly reviewing and altering investment strategies in FI. The current study illustrates the regulatory compliance with AI in financial sectors, including the banking system. The present study highlights challenges, risks, and regulatory compliance status involving AI in the financial sector.

The existing study (Lee & Chen, 2022) determines the user's intention to adopt the evolution of AI mobile banking and explores factors that influence the user's intention in banking. The outcome of the prevailing study indicated anthropomorphism and intelligence are the factors, and this finding provides practical guidance for banks to utilize AI for customer retention. The current study demonstrated the significant role of regulatory compliance, including challenges, strategies, beneficiaries, and risks with AI in the financial and banking sectors.

The existing study (Burgt, 2020) illustrates the explainable AI in the banking sector and highlights the importance of understanding the techniques and risks when assessing different situations. The prevailing study proves trust is an important, challenging factor in banking. The current study discussed the regulatory

compliance and risks involved with AI in banking. The results of the present study emphasize regulatory compliance with AI as a crucial factor and data privacy as a major risk in banking with AI.

Conclusion and Future Recommendations

Technology changes have altered how corporate industries progressed along with consumers. With the evolution of technologies and users' growing expectations for a digital arrangement with FI, Banks need to align and adopt emerging AI technologies that support efficiency, security, accuracy, and speed. The financial sector changes rapidly because of increasing digitalization, and banks adapt to new technologies to keep up with changing customer needs, experiences, and behaviors. Therefore, the present study analyses the influence of AI in the investment sector and its advantages. Banking is a highly regulated industry of the economy worldwide; as AI and the financial sector integration grows, the significance of addressing issues increases. Regulatory compliance with AI and risks involved in finance are deliberated to understand legal compliance. So, the current study analyzed regulatory compliance with AI. In addition, the study also investigated the challenges related to AI in the financial sector, such as lack of transparency, data privacy, and security. The present study recommends a robust regulatory framework, frequent security checks, privacy policies, and highly technical solutions to overcome the challenges of adopting AI.

References

[1]. Alzubaidi, L., Al-Sabaawi, A., Bai, J., Dukhan, A., Alkenani, A. H., Al-Asadi, A., . . . Albahri, A. (2023). Towards risk-free trustworthy artificial intelligence: Significance and requirements. International Journal of Intelligent Systems, 2023.

[2]. Ashta, A., & Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. Strategic Change, 30(3), 211-222.

[3]. Burgt, J. v. d. (2020). Explainable AI in banking. Journal of Digital Banking, 4(4), 344-350.

[4]. Carmody, J., Shringarpure, S., & Van de Venter, G. (2021). AI and privacy concerns: a smart meter case study. Journal of Information, Communication and Ethics in Society, 19(4), 492-505.

[5]. Chadha, P., Gera, R., Khera, G., & Sharma, M. (2024). Challenges of Artificial Intelligence Adoption for Financial Inclusion Artificial Intelligence, Fintech, and Financial Inclusion (pp. 135-160): CRC Press.

[6]. Elliott, D., & Soifer, E. (2022). AI technologies, privacy, and security. Frontiers in Artificial Intelligence, 5, 826737.

[7]. Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. Technological forecasting and social change, 163, 120407.

[8]. Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges, and future research directions. Expert Systems with Applications, 240, 122442.

[9]. Hobvi, A. L. J., Zunaidi, A., & Fikriyah, A. (2022). Implementation Of Compliance Management In The Sharia Banking Sector. Proceedings of Islamic Economics, Business, and Philanthropy, 1(2), 346-362.

[10]. Hu, B., & Wu, Y. (2023). AI-based compliance automation in commercial bank: how the Silicon Valley Bank provided a cautionary tale for future integration. International Research in Economics and Finance, 7(1), 13.

[11]. Hyder, Z., Siau, K., & Nah, F. (2019). Artificial intelligence, machine learning, and autonomous technologies in the mining industry. Journal of Database Management (JDM), 30(2), 67-79.

[12]. Janssen, M., Weerakkody, V., Ismagilova, E., Sivarajah, U., & Irani, Z. (2020). A framework for analyzing blockchain technology adoption: Integrating institutional, market and technical factors. International journal of information management, 50, 302-309.

[13]. Kitsios, F., Giatsidis, I., & Kamariotou, M. (2021). Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. Journal of Open Innovation: Technology, Market, and Complexity, 7(3), 204.

[14]. Königstorfer, F., & Thalmann, S. (2020). Applications of Artificial Intelligence in commercial banks–A research agenda for behavioral finance. Journal of Behavioral and Experimental Finance, 27, 100352.

[15]. Kumar, D., & Suthar, N. (2024). Ethical and legal challenges of AI in marketing: an exploration of solutions. Journal of Information, Communication, and Ethics in Society.

[16]. Lee, J.-C., & Chen, X. (2022). Exploring users' adoption intentions in the evolution of artificial intelligence mobile banking applications: the intelligent and anthropomorphic perspectives. International Journal of Bank Marketing, 40(4), 631-658.

[17]. Lupo, G. (2023). Risky Artificial Intelligence: The Role of Incidents in the Path to AI Regulation. Law, Technology and Humans, 5(1), 133-152.

[18]. Malali, A. B., & Gopalakrishnan, S. (2020). Application of artificial intelligence and its powered technologies in the Indian banking and financial industry: An overview. IOSR Journal Of Humanities And Social Science, 25(4), 55-60.

[19]. Mbaidin, H. O., Alsmairat, M. A., & Al-Adaileh, R. (2023). Blockchain adoption for sustainable development in developing countries: Challenges and opportunities in the banking sector. International Journal of Information Management Data Insights, 3(2), 100199.

[20]. Mogaji, E., & Nguyen, N. P. (2022). Managers' understanding of artificial intelligence in relation to marketing financial services: insights from a cross-country study. International Journal of Bank Marketing, 40(6), 1272-1298.

[21]. Mohsen, S. E., Hamdan, A., & Shoaib, H. M. (2024). Digital transformation and integration of artificial intelligence in financial institutions. Journal of Financial Reporting and Accounting.

[22]. Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. arXiv preprint arXiv:2102.04661.

[23]. Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. International Research Journal of Modernization in Engineering Technology and Science, 5(9), 128-137.

[24]. Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: an empirical analysis. International Journal of Emerging Markets, 18(10), 4270-4300.

[25]. Rohada, N. (2023). Application of Artificial intelligence in financial services. from https://www.linkedin.com/pulse/applications-artificial-intelligence-financial-sector-neelam-rohada

[26]. Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. Law, Innovation and Technology, 13(1), 57-84.

[27]. Thowfeek, M. H., Samsudeen, S., & Sanjeetha, M. B. F. (2020). Drivers of artificial intelligence in banking service sectors. Solid State Technology, 63(5), 6400-6411.

[28]. Watson, T. (2021). The large bank had a compliance challenge. from https://www.amitracks.com/large-bank-had-a-compliance-challenge/

[29]. Yanting, Z., & Ali, M. (2023). Artificial Intelligence, Digital Finance, and Financial Inclusion: A Conceptual Framework Financial Inclusion Across Asia: Bringing Opportunities for Businesses (pp. 77-85): Emerald Publishing Limited.

[30]. Yu, T. R., & Song, X. (2021). Big Data and Artificial Intelligence in the Banking Industry Handbook of Financial Econometrics, Mathematics, Statistics, and Machine Learning (pp. 4025-4041): World Scientific.

[31]. Zhu, H., Pysander, E.-L. S., & Söderberg, I.-L. (2023). Not transparent and incomprehensible: A qualitative user study of an AI-empowered financial advisory system. Data and Information Management, 100041.

[32]. Zulfikar, R., Lukviarman, N., Suhardjanto, D., Ismail, T., Dwi Astuti, K., & Meutia, M. (2020). Corporate governance compliance in the banking industry: The role of the board. Journal of Open Innovation: Technology, Market, and Complexity, 6(4), 137.