ARTIFICIAL INTELLIGENCE IN DIGITAL BANKING: NAVIGATING IMPLEMENTATION BARRIERS

Dr. Sunita Sikri*; Dr. Ashok Khurana**

*Associate Professor,
Department of Commerce,
MLN College, Yamuna Nagar,INDIA

**Associate Professor,
Department of Commerce,
Guru Nanak Khalsa College, Yamuna Nagar, INDIA

DOI: 10.5958/2249-7137.2024.00034.9

ABSTRACT:

This study explores the challenges faced by the banking sector in implementing Artificial Intelligence (AI) technologies, focusing on factors such as Malicious Uses of AI, AI Model Theft, Lack of Transparency, Adversarial Attacks, Digital Banking Applications, and Data Analysis. Through regression analysis, the study examines how these challenges influence the improvement of business data models within the banking industry. The data was collected from 733 respondents using convenience and judgement sampling methods. The results indicate that Lack of Transparency has the most significant positive effect on the improvement of business data models, suggesting that addressing transparency issues in AI systems is crucial for better AI integration in banking. Data Analysis and Adversarial Attacks also show significant, albeit smaller, positive relationships with business data models, emphasizing the importance of robust data systems and defence mechanisms against adversarial manipulations. Conversely, AI Model Theft and Malicious Uses of AI showed relatively weak and non-significant effects on business data models, though they are still recognized as important concerns. The findings highlight the critical role of transparency, data analysis, and security in AI adoption in the banking sector, offering valuable insights for practitioners and policymakers. The study concludes with practical recommendations to mitigate these challenges and enhance AI-driven business processes in banking.

KEYWORDS: *Transparency, Emphasizing, Improvement, Integration, Adoption.*

INTRODUCTION

Digital banking has taken off and transformed the financial services landscape with a level of convenience, accessibility and efficiency we have never seen. The cascading of this transition is on multiple fronts of Artificial Intelligence (AI) application integrations. Therefore, AI solutions help boost the client experience, make decision making a priority, and eliminate many operations in the financial system. While AI applications promise much, the digital banking sector confronts unique barrier to the adoption and deployment of these technologies for use safely and effectively. Over the past few years, digital banking has exploded, and it has a lot to do with AI – driven technologies (Arora et al., 2020). Digital banking systems can take advantage of AI to provide custom services, make better decisions, reduce running costs and increase security. Yet, the obstacles are immense to the adoption of AI technologies through digital banking. Banks, regulators, and clients all have cause to be worried about the harmful application of AI, issues of transparency, and security (Goodfellow et al., 2014).

The increasing number of banking systems that now have AI integrated into them are beginning to show their vulnerability. The AI can be utilized to generate disinformation, support a cyberattack, commit a fraud and more. (Binns et al., 2021). The destructive acts of these threats to digital banking are a threat to the confidence that digital banking can bring and the security that goes with the use of digital banking and it, therefore, requires a lot of governance and regulatory procedures to curb such malicious acts. Thus, that’s exactly what it is as digital banking systems become more advanced and turn to AI to manage sensitive consumer data and transactions (Chesney & Citron, 2019). One of the biggest concerns with AI is the sinister potential uses of it for pumps of disinformation, hacks and fraud. The danger that AI generated deepfakes pose to client confidence and security in today’s digital banking systems is immense. (Dastin et al., 2022).

The issue with the use of AI in digital banking is considerable due to theft of AI models. However, unlike traditional intellectual property protection approaches, AI models do not adequately protect these resources as a proprietary asset. As a result, digital banks are vulnerable to theft, leaving modern banking technologies open to be replicated or reverse engineered by unauthorized third parties. Deceit of this nature can be very costly and can drain the bank's competitive advantage, stifling innovation in the banking sector in terms of creativity, establishment of networks and competition (Dong et al., 2021). Although encouraging the adoption of open-source AI models toward cooperation and accessibility, the rapid distribution of these models simultaneously enlarges the space for malicious application. Thus, digital banks require strong methods for securing their AI models from theft using encryption, licensing (intellectual property) or other intellectual property protective methods (Goodfellow et al., 2015).

The lack of transparency in AI systems is a big barrier to AI use in digital banking. However, decisions made by many AI models are sometimes referred to as black boxes which means that we don’t have clear understanding of the reasons behind them. A combination of explainability and transparency can mitigate the consumers or other stakeholders’ scepticism when AI systems used for activities such as loan approvals, risk management and fraud detection. Banks should develop strategies that help make their AI models transparent to the customer since these systems are affecting the material well-being of itself (Lipton, 2018). The theft of AI models could hurt their unique competitive advantage and future innovation. If different open-source AI models continue to advance in continuous manner to be deployed in different application environments then these may introduce new type of security vulnerabilities not discussed in conventional security literature. This lack of transparency undermines trust in digital banking systems and carries huge risks with respect to accountability for decisions that can impact individual and enterprise financial health and wellbeing (Chen et al., 2020).

Adversarial attacks on AI systems are becoming more and more of a serious threat. Such AI assaults have become currently accessible which includes, using the use of AI models to produce inaccurate and biased results leading to significant compromise of the digital banking system's reliability. The problem is that, in high stakes domains like finance and healthcare, AI driven banking services can become less efficient due to the hostile inputs. Without the proper security measures to protect against these threats, digital banking systems are inherently exposed to a massive number of risks. Adversarial attacks in digital banking raise an additional issue with the security and dependability of AI (Binns et al., 2021). In this situation, these attacks alter the input in such a way that trick the AI model into making wrong or wrong predictions. In an industry as sensitive as canvas even minor inaccuracies in the system can have to catastrophic consequences. For example, depending on system configuration, hostile inputs could compromise a fraud detection system or cause an AI driven credit scoring model to make the wrong choices. Because AI systems are set to become embedded deeply within the digital banking process, hostile attacks become riskier than ever (Zhang & Wu, 2021).

The financial sector must protect itself from these assaults and impose stringent security policies, including intensive testing, a defensive strategy, and real time surveillance, so the AI models are equipped to survive enduring and orchestrated manipulations. Usage of AI in digital banking is predicted to increase and associated worries will develop regarding data safety and privacy protection. In an age of data intensive AI systems, they are vital assets that require banks to protect and closely watch transfer of data. When it comes to digital banking business, the most troubling issues are data breach, hacking attack and unlawful access to the personal information of the clients. However, banks have been making tremendous strides in their approach to cyberattacks and the AI driven banking systems have no choice but to compete with the most recent technologies available in order to compensate for such potential risks (Goodfellow et al., 2015).

With this transformation of digital banking, banks, financial institutions, and regulators all need to come together to address these issues. To mitigate the risks involved, banks have to do all of the above, as they need to ensure that the system is thoroughly tested and secure, while also providing full transparency and in instances where IP is ditched, protect it adequately (Kshetri, 2020). Only a balanced strategy can help realize the complete potential of AI and provide for a safer and improved future digital banking systems. The potential integration of AI has the potential to significantly benefit the digital banking sector, as well as there are some challenges that need to be met for an improved potential of this sector. (Patel, 2021). For AI to be used fairly, securely and transparently in the banking sector, then financial institutions, regulatory agencies, banks and technology providers must collaborate together to put in place necessary safeguards.

Literature Review

Digital banking is surprisingly fast to implement Artificial Intelligence (AI) with a range of AI technologies to automate processes, help make better decisions and heighten customer experience. Fraud detection, digital assistants, personalized suggestions, predictive analytics: There are different applications of AI. In addition, AI offers many exciting things for positive outcomes if it is used discreetly in the digital banking industry, which has a lot of challenges. In turn, most of the challenges related to these challenges are concerning information security, transparency, intellectual property, and the ethical use of AI (Adadi & Berrada, 2018). Digital banking uses artificial intelligence (AI) more and more to automate processes, improve decision-making, and further improve the customer experience through each of the different kinds of AI technologies listed in the preceding chapter. The fraud detection, personalized suggestions, digital assistants and even predictive analytics are applications of AI. However, implementation of AI at digital banking is a complex process. The main problems are in the field of security, transparency, intellectual property and the use of AI (Raji & Buolamwini, 2019). The purpose of this literature review is to discuss the main issues digital banks reflect in using AI as their inherent responsiveness to uptake AI poses a major security challenge: malicious use of artificial intelligence, theft of AI models, lack of transparency and adversarial attack on artificial intelligence.

E-Banking Malicious Applications of Artificial Intelligence

The implementation of AI technology in digital banking faces a significant challenge. The addition of AI in the banking system makes them more vulnerable to such things like malicious attacks and risky operations. AI technologies may use deep learning and natural language processing artifacts improperly to create advanced forms such as phishing, social engineering, and fraud (Brynjolfsson & McAfee, 2017). Mitsis (2018) establishes deepfake technology as technology that can create synthetic video and audio within the domain of replication of an individual's voice or appearance which Chesney and Citron (2019) note as a big security to banking institutions. A concerning use of deepfakes is for people to pretend to be they are bank workers or clients.

However, due to AI's ever-increasing role in digital banking the potential for harm increases. As AI algorithms now allow fraudsters to foretell consumers' behaviour, search for system vulnerabilities or increase the efficiency of phishing (Chesney and Citron, 2019). Just like any other tool, AI systems can mimic human interactions, and hence appear as genuine individuals to clients, deceiving them into disclosing sensitive information like account numbers and passwords. The problem data breaches pose is huge when you consider the costs involved for breaches to digital banking. Banks are concerned about the ethical implications of using AI to detect and prevent fraud because it is necessary to combine privacy with effective detection for efficient AI driven security solutions, as highlighted by (Kshetri 2020). In that case, banking entities will spend large sums securing technologies designed to prevent AI misuse and develop AI solutions in an extremely secure way. As AI is founded on these financial markets, it will be bound for taking actions that manipulate financial markets or misinform clients, with huge repercussions for banks. Misinformation from AI can destroy client confidence and trust leading to the panic of withdraw and financial instability (Aked, 2016). Digital banks are, in themselves, a conduit for hostile actors to exploit and digital banks need to make stricter security measures for these technologies. Governments and investment institutions must together create legislation which would set vigorous controls on the use of bots in financial services to prevent risks. Binns, 2018.

Theft of models by artificial intelligence

The deployment of AI applications by digital banks is a prime focus of concern given the risk of AI model theft, which can undermine the competitive benefits of their unique AI technologies. Unauthorized duplication and use of proprietary AI models can serve to undermine the marketplace of proprietary AI models and disrupt the trustworthiness of the AI ecosystem. There has been a lot of talk on this topic and many more banking institutions are now trying to employ machine learning (ML), algorithms that take up a lot of time, money, and data to develop. The theft of intellectual property can cause losses of enormous financial amounts for companies in the banking sector and other sectors (e.g. Brown & Grant, 2019; Chan et al., 2019). In the setting of deep learning models, such theft is so prevalent that the model can become completely broken. Digital banks would suffer from catastrophic theft of AI models because these models are proprietary and have a competitive advantage in credit scoring, fraud detection and customer care. Or how do you protect the AI models at the core of digital banking systems—models that are becoming more and more important to those banking systems—from being replicated and misused? Digital banks put a lot of money into investing in developing AI models — competitive edge is credit scoring, fraud detection, customer service automation, etc. However, an issue exists: There has been no comprehensive intellectual property protections established for AI models. Dissemination of AI models happens often as open–source or from a cross–platform (Zhang et al., 2021) which carries the risk of unlawful duplication.

Theft of an AI model erodes digital banking institutions' competitive advantages and discourages AI innovation investment (Shin, 2019). Safe and enforceable intellectual property rights do not exist in digital banking organizations' case which could make these organizations hesitant to fully take advantage of AI because of a threat to lose their proprietary models. Secondly, the fact that AI models are open source and therefore used, for instance, to cut operational expenses or promote innovative activity, makes them the target of malicious people (LeCun et al., 2015). These implications apply to the secured deployment of AI within the financial sector. In fact, solid guarantees against AI model theft will certainly help keep the AI motion in digital banking on track. This issue however has been worsened by the proliferation of open-source AI models, since they can be effortlessly integrated into many digital financial systems unregulated and without protective measures like requisite authorization. Consequently, digital banking firms are prey to hostile actors stealing their intellectual property by using open-source AI technologies (Patel, 2021). For a bank to be able to maintain its innovation and technological superiority, intellectual property of AI driven apps must be protected.

Invulnerable nature of AI systems

The big obstacle to the widespread adoption of AI in the digitization of banking is the lack of transparency in the AI decision making process. Many AI models, especially deep learning models as well as 'black box' AI models, are not easily interpretable or decipherable to humans, and especially not their decision-making processes related to resulting outcomes for humans (Raji, Keswani & Selvaraju, 2020). Absence of transparency in AI driven banking application can break client and stakeholder trust by giving opportunities to unethical practices. In banking organizations, a lack of transparency in AI systems brings a missing piece of accountability for the clients to understand and challenge decisions such as loan approvals, credit score, and fraud alarms. The issue of AI transparency is a critical challenge facing banking, as it means banks that employ AI bear responsibility for this AI and must preserve confidence. As Burrell (2016) pointed out that client demands for clarity are very high when it comes to the digital banking financial sector, especially around credit scoring, loan acceptance and fraud detection, when they expect a very high degree of transparency. By failing to publicly broadcast the reasoning of AI systems, public confidence in digital technological financial platforms is undermined and the fairness of those systems is rendered less believable (Raji & Buolamwini, 2019).

According to a number of experts, openness is a key ingredient in building trust between digital financial organizations and their users. If customers cannot be transparent in their decision making processes in AI driven banking systems, they may opt to not use them fully (Dastin, 2018). Academics propose that in response to the problem of explainability, banks should understand how to explain their AI models to increase transparency (Gilpin et al., 2018). AI systems should offer transparent and trustworthy, and reliable explanations of decisions to clients, thus engendering trust and fairness in the treatment of clients. One well known example of banking AI opacity is the use of automated credit scoring systems which have been criticised for being non-transparent and unaccountable. However, these systems mostly rely on elaborate algorithms to determine one's credit standing, which causes a problem of biased discrimination and unjust loan rejections (O'Neil 2016). Calls for the regulation of AI operations in financial services lack transparency in AI decision making it necessary to have a framework which is more interpretable, responsible and aligned with consumer protection standards (Bryson et al., 2017).

Regulatory compliance requires transparency in AI models. As the reliance on AI systems to make financial decisions goes up, regulators require a deeper understanding of operational mechanisms of AI systems. In some jurisdictions, financial institutions may be required to prove that their AI systems meet compliance with fairness and anti discrimination legislation (Anderson 2021). As a result, frameworks to apply AI auditing and explanations are built to ensure digital banks are compliant and can prevent biases and discriminatory results during the usage of AI technology (Mehrabi et al., 2019).

Adversarial attacks

The second dangerous risk of AI in the digital banking space is the adversarial attack. Adversarial attacks use a malicious user's ability to craft input data so as to trick a system under the impression it is an AI. In banking, adversarial attacks can perturb on systems such as fraud detection, client verification, or credit scoring with detrimental financial performance impacts (Goodfellow et al., 2015). These attacks are possible because the AI algorithms — and in particular machine learning models — that rely on large amounts of training data for their functioning are vulnerable by nature. For example, such perpetrators can intentionally manipulate/stage transaction data to work around fraud detection systems, and that would lead to undetected fraudulent transaction. Adversarial attacks are hard on digital banks with AI systems. An adversarial attack, as defined here, is an attack on the input data of an AI model in a method so that the AI model makes incorrect predictions or conclusions. Such attacks cripple the performance of AIs in such important areas like fraud detection, transaction verification, and risk assessment. In the financial and healthcare industries where these attacks are particularly alarming, because they can have a major impact on customers and companies alike (Goodfellow, 2015). Adversarial inputs can cause misclassified fraudulent transaction, incorrect loan decisions and weaknesses in AI based authentication in digital banking.

Because of the risks linked with adversarial attacks, there has been significant research as how digital banks could further strengthen the security of their AI systems. There have been several proposed defensive strategies, such as adversarial training of AI models, training the models using hostile inputs to make them robust to such inputs (Tramèr et al., 2017). However, many digital banks are still ineffective at detecting and combating attacks against their AI systems (Papernot et al., 2016). The most perilous banking sectors are payment processing and identity verification, most vulnerable to adversarial applications doing the most damage. The attack on such systems may lead to large scale disruption, financial losses and damage to the reputation of digital banking institutions (Papernot et al., 2017). In turn, banks will have to be willing to make significant investments into advanced security protocols, including rigorous training of bank personnel in adversarial techniques, incorporating adversarial training techniques into our system, to ensure that our AI driven solutions can stand up to such attacks.

AI in digital banking poses many things to be taken care of to implement AI would work and ensures security of the process, too. There are many challenges in digital banking, some bad uses of AI, theft of AI models, lack of transparency and adversarial attacks. In order to address these three concerns, digital banks would need to team up with regulators and researchers to build secure, more transparent and explicable AI systems. Additionally, banks need to establish stronger defence mechanisms against the adversarial attacks in order to prevent AI risks, as well as establish enhanced intellectual property rights. While this will push the advancement of AI, the problem of preserving reliability, security, and confidence will become a more significant problem in digital banking systems (Anderson, 2021).

The key objective of this research is to examine the challenges faced by the digital banking entities in the use of AI applications for its rollout both harmfully and theft of AI models, inadequate transparency, and adversarial attacks. Here we study the impact of these problems to security, creativity, and reliability of the digital banking systems. According to the literature, banks must increase cybersecurity protocols, improve AI model transparency, and shield their intellectual capital (Papernot et al., 2016). The project contemplates exploring some proposal for legislations that may solve these problems so that the use of AI technology in the digital banking sector occurs in a modality that is responsible and ethical (Brynjolfsson & McAfee, 2017).

The goal of this research is to offer practical advice to digital banks to enhance the integrity of their AI applications to alleviate security, transparency and resilience to malicious exploitation and adversarial manipulation. Literature substantiates the aims of looking at these issues being confronted to ensure the longevity and growth of AI driven digital banking systems. Digital banks can better protect the system, engage in trust building among their clients, and maintain a competitive advantage as the importance of AI in the financial sector continues to grow by understanding these threats and fashioning proactive remedies.

Hypothesis

Based on the objectives outlined, the following hypotheses can be formulated to guide the research on the challenges faced by digital banking in implementing AI applications:

Hypothesis 1: The Malicious Use of AI has significant impact on the Digital Banking applications.

Hypothesis 2: AI Model Theft has significant impact on the Digital Banking applications.

Hypothesis 3: Lack of Transparency in AI Decision-Making has significant impact on the Digital Banking applications.

Research Methodology

In this study, researcher has investigated the challenges facing digital banking in deploying AI applications around concerns such as the nefarious usage of AI, theft of AI models, and opaque AI systems. Factor Analysis and Regression Analysis will be applied in the study to analyse the data collected from 733 respondents in sample. The method of convenience sampling will be applied to obtain the easiest accessible individuals for instance individuals who are utilizing digital financial services. To get a more representative sample of the community who are the digital banking customers, judgement sampling is used to collect data from them.

A standardized questionnaire using both closed and open-ended questions is used to gather data pertaining to the problems with the deployment of AI in Digital banking. Online survey will be sent to the randomly selected respondents. The use of Factor Analysis will help to identify the underlying characteristics that impact the obstacles of the application of AI in digital banking. The impact of listed factors for utilizing AI applications in the banking sector will be analyzed through regression analysis. Data processing and analysis will be done with statistical software SPSS. The results from this methodology will be quantitative, which will lead to opinions about the challenges of AI in digital banking.

Data Analysis

The demographics contain a high level of detail regarding the study's respondents, including gender, age, educational level, marital status, and profession. The sample comprises 733 respondents, with a rather equitable gender distribution such as 52.5% male and 47.5% female. Age range is distributed over a wide age range, as predominance is 40-50 years (25%), 30-40 years (22.9%) and 20-30 years (21.1%) whereas 12.4% are individuals over 60 years, thus representing generalised demographics. Respondents have graduated at the highest rate (32.1%), followed by under graduates (21.1%), post graduates (19.1%) and those who have done education beyond post graduate level (7.5%). According to marital status, 40% of respondents are married and 38.3% unmarried whereas in case of occupation, professionals are the most dominant (28.2%) group followed by private sector employees (23.1%), entrepreneurs (19.4%), public sector workers (14.7%) and self-employed (14.6%). The statistical nature of occupational variety means that the data is broad enough and representative enough to sample different demographics to examine the issues of AI in banking.

Table 1 Profile of factors affecting the implementation of AI applications in Digital banking system

Construct	Cronbach's alph	Eigen values	Items	Factor loadings
Adversarial Attacks	.832	6.162	5	.914 to .754
AI Model Theft	.796	3.145	5	.850 to .716
Data Analysis	.784	2.882	5	.804 to .738
Lack of Transparency	.805	2.245	3	
Digital Banking Applications	.724	1.515	3	.913 to .617
Malicious Uses of AI	.626	1.348	3	.898 to .770
(Total Variance Explained= 72.07, KMO= .815, Bartlett’s test = .000)				

Source: Primary Data

Table 1 presents that cronbach's alpha values clearly show strong internal consistency in all constructs, from 0.626 (Malicious Uses of AI) to 0.832 (Adversarial Attacks), among which we see that our constructs are reliable. Once all the components contribute significantly to the total variance, that is, the eigenvalues are greater than 1. The model explains a total of 72.07% of the data’s volatility. The Kaiser-Meyer-Olkn (KMO) value of 0.815 and the significant (p = 0.000) Bartlett’s test show that the data is acceptable for factor analysis. The items all load robustly on their corresponding factors, ranging in factor loadings from 0.617 to 0.914.

Table 2 Mean score comparison for different challenges faced by banking sector by implementing AI based on the education of the respondents

	Under Graduate	Graduate	Post Graduate	Above Post Graduation	Others	Total
Malicious Uses of AI	3.8172	3.8993	3.9381	3.8364	3.9685	3.8986
AI Model Theft	3.9213	3.8511	4.0057	4.0909	3.9014	3.9236
Lack of Transparency	3.6984	3.8085	3.8625	3.5500	3.7973	3.7739
Adversarial Attacks	3.7845	3.7881	3.8400	3.6691	3.7811	3.7869
Digital Banking Applications	3.6753	3.7986	3.9095	3.6121	3.7027	3.7603
Data Analysis	3.8116	3.8570	3.8157	3.8836	3.8608	3.8423

Source: Primary Data

Table 2 presents a comparative analysis of the problems faced by the banking sector in the implementation of AI is made by comparing the mean scores for each problem, according to the educational level of the respondents. Malicious uses of AI are acknowledged universally across all educational demographics but have a marginally higher level of awareness by post graduate and above (3.9381), meaning that there is more awareness in security threat among respondents having educational level above post-graduation. Those with postgraduate degrees or higher (4.0909) viewed AI Model Theft as the most symptomatic concern suggesting that higher educational attainment is correlated with greater awareness in regards to the perils of intellectual property theft within the AI technology. On the contrary, Lack of Transparency (3.5500) sees the largest fall in the postgraduate group, perhaps indicating that the participants' higher education translated into them having higher confidence in AI systems or greater ability to comprehend the underlying transparency problems. Average responses for adversarial attacks and enhanced business data models show generally equal feedback across groups, showing a similar level of concern regarding all levels of education about these topics. Lastly, in the case of data analysis, people from different educational backgrounds share the same views, which means data driven decision making is crucial for implementation of AI. This study shows that respondents' perceptions of problems in AI deployment change with educational attainment, with the more educated respondents reporting higher levels of awareness for particular problems such as AI model theft.

Table 3 ANOVA test statistics for the different challenges faced by banking sector by implementing AI based on the education of the respondents

Test of Homogeneity of Variances						
	Levene Statistic	Sig.	Statistic[a]	Sig.	F	Sig.
Malicious Uses of AI	.461	.765	1.470	.212	1.559	.183
AI Model Theft	3.436	.009	2.498	.043	2.047	.046
Lack of Transparency	.710	.585	2.758	.028	2.623	.034
Adversarial Attacks	.992	.411	.662	.619	.707	.587
Digital Banking Applications	6.102	.000	2.528	.041	2.539	.039
Data Analysis	1.113	.349	.318	.866	.290	.884

Source: Primary Data

The table 3 presents the results of test of homogeneity of variances for educational level of respondents and issues on banking industry AI implementation issues are significant and non-significant variances across parameters. There is a significant result for AI theft model, lack of transparency and digital banking applications, which means respondents are more worried about concerns related to AI abuse based on these factors with respect to their educational levels and possess diverse observations for these factors. The Levene statistic provide insignificant results for malicious use of AI, adversarial attacks and data analysis factors, indicating that all the respondents perceive similar perceptions for these factors based on their educational levels.

Table 4 Regression Model for different challenges faced by banking sector by implementing AI based on the education of the respondents

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.432[a]	.186	.181	.71474	.186	33.303	5	727	.000	1.903
a. Predictors: (Constant), Data Analysis, Adversarial Attacks, AI Model Theft, Lack of Transparency, Malicious Uses of AI										
b. Dependent Variable: Digital Banking Applications										

Source: Primary Data

Regression model shows moderate positive relationship between AI implementation problems and digital banking applications (R = .432, 18.6% of variance explained, R2 = .186). The adjusted R² (.181) confirms the reliability of the model as variables like Data Analysis, Adversarial Attacks, AI Model Theft, Lack of Transparency and Malicious AI Uses do not have a considerable impact on digital banking applications. Standard error (.71474) implies prediction error and the F value (33.303, $p < .000$) asserts adequacy of model. Durbin-Watson statistic (1.903) also support the model as no residual autocorrelation exist. Although the impact of the predictors is significant, overall, their impact is moderate and thus the other elements of the business data model need to be studied.

Table 5 Regression coefficient for different challenges faced by banking sector by implementing AI based on the education of the respondents

Coefficients[a]							
Model		Unstandardized Coefficients		t	Sig.	Collinearity Statistics	
		B	Std. Error			Tolerance	VIF
1	(Constant)	1.137	.256	4.435	.000		
	Malicious Uses of AI	.088	.051	1.739	.082	.777	1.287
	AI Model Theft	.209	.040	.223	.024	.926	1.08
	Lack of Transparency	.376	.041	9.158	.000	.846	1.183
	Adversarial Attacks	.291	.043	2.113	.035	.905	1.104
	Data Analysis	.125	.051	2.475	.014	.721	1.387
a. Dependent Variable: Digital Banking Applications							

Source: Primary Data

The statistical significance and multicollinearity of each predictor variable’s contribution to digital banking applications is shown in the Coefficients table 5. At zero predictors, the constant (B = 1.137) is highly significant (t = 4.435, p < .001), thus providing a good baseline for digital banking application model. Malicious Uses of AI (B = .088, t = 1.739, p = .082) is positively related with digital banking applications (marginally significant at the .05 level which implies that these other variables have a stronger effect). We find that AI Model Theft (B = .209, t = .223, p = .024) has a statistically significant positive effect on digital banking applications, suggesting that the threat of intellectual property theft may cause businesses to improve data models, perhaps because of greater emphasis on protecting AI innovations. Transparency concerns show a substantial positive correlation with corporate data model improvement (B = .376, t = 9.158, p < .001). We found that Adversarial Attacks (B = .291, t = 2.113, p = .035) and Data Analysis (B = .125, t = 2.475, p = .014) have significant impact on the digital banking applications. The results indicate that transparency, adverbial attacks, and AI model theft have the highest impact or poses major challenges in the smooth running of digital banking applications whereas malicious uses of AI and data analysis has the significant but least impact on the implementation of digital banking applications. The Tolerance and VIF values do not have high level of multicollinearity indicating these predictors are not correlated with each other too much which allowed us not to have highly unstable and unreliable regression coefficients.

Discussion

In this study, we examined current banking industry issues and impact on business data models when applying AI. As banking begins to integrate AI, it’s critical to understand the elements that drive AI adoption and optimization for efficiency, security, and competitiveness. Criminal AI use, AI model theft, transparency issues, adversarial attacks, and how data analysis enhances business data models were addressed by this study. As evidenced in the previous sections’ regression study, there is a complex relationship that banking AI adoption has on these challenges. Large and marginally important ways that banking business data model advancements are affected by Malicious Uses of AI, AI Model Theft, Lack of Transparency, **Adversarial Attacks, Data Analysis**

The slightest improvement was seen in Business Data Models, with malicious AI use. The coefficient of .088 is in particular not standardized, and indicates that while concerns about malicious AI use marginally raise the level data model upgrades, its significance level of .082 means that such an effect is much weaker than other predictors. This marginal relevance may suggest the banking sector is increasingly concerned about AI plunder, fraud and disinformation, and is looking to prevent such. Data leaks and harmful AI use are security risks of AI that worry the world. In fact, as AI becomes more common in banking, cyberattacks, identity theft and fraud are also rising (Zhou et al., 2021). This is recognized; however, the exact continuous danger or attack is not necessary for improvement in the business data model until now (Sarker et al., 2020). To make this worse, such dangers should be reduced, with strong cybersecurity protocols and AI based fraud detection systems (Binns et al., 2021).

Finally, AI Model Theft also positively and statistically significantly (B = .209, p = .024) impact digital banking applications. Protecting intellectual property in AI applications is crucial to the AI models, since models are proprietary in the digital world and therefore can be treated as a valuable commodity. As AI model theft concerns rise, the banking sector will put data model improvement at the top of its priority list with this coefficient. Thieves can steal proprietary AI models resulting in massive financial and intellectual property damage and losses that can kill organizations competitive edge (Zhou et al., 2021). Since AI models are used for customer service automation, risk management and fraud detection in banking, theft or unauthorized replication of them can cripple innovation and security. In support of previous research towards encryption (Dastin et al., 2022), these findings advocate for encryption, as well as other protections required to make AI models secure for innovation.

The strongest significant positive correlation between Lack of Transparency and digital banking applications was B = .376, p < .001. In banking, AI process transparency is key. Typically, AI systems are "black boxes"—hard to understand decisions may erode customer and regulator trust (Kroll et al., 2017). Highlighting this relevance puts the issue of AI explainability and openness on the rise. For regulatory compliance and customer trust in banking, transparency is a key, as AI models determine whether to approve a credit, transfer money, or detect whether an online transaction is fraudulent (Zhou et al., 2021). The banking sector also calls for model transparency standards such as explainable AI (XAI) in the case where AI is integrated in the fundamental banking processes, to explain the AI system's decision making.

Worries about AI model sensitivity to adversarial manipulations statistically significantly motivated commercial data model enhancements (B = .291, p = .035, Table 2). Adversarial assaults that tweak input data to fool the AI systems can be particularly destructive in sensitive industries such banking (Goodfellow et al., 2014). The banking sector is aware that the problems of vulnerability to adversarial input exist and is already employing more advanced means to protect against such inputs. This finding is consistent with the ongoing research on AI security that requires the development of strong defenses such as adversarial training in high stakes AI deployments (Papernot et. al, 2016).

Business data model improvements were also predicted by Data Analysis (B = .125, p = .014). AI succeeds in banking because AI systems are best for patterns and data analysis, and with banking, you need to store, analyze, and use data for decisions in enormous amounts, at least when it comes to clients and transactions. According to the positive coefficient, greater amount of data analysis results in better AI model building. As AI systems become more embedded in business operations, from banking in particular (Chen et al., 2020), much more needs to be done in order to optimize AI applications, which requires data analysis on a massive scale. Better data models mean better data driven banking decision, such as in improving customer service, risk management and fraud detection (Zhou et al., 2021).

Future implications

Several major implications for banking AI adoption and optimization are presented in this study. Worries about malicious AI use are important, but have less influence in enhancing business data models than issues like transparency or theft of AI models. Opening, fairness and explainability should also be prioritized in AI deployment in banking, even as cybersecurity and anti fraud policies are key. Strong IP protection is also needed because of AI Model Theft. Banks have to protect AL models from theft and reproduction. Since the efficiency of AI models and business decisions critically depends on data analysis, banks should invest in it. The need for banking AI security is also shown by Adversarial Attacks. Once AI enters the industry fraud and risk inference, as well as consumer interaction, the industry must make sure that the AI system is robust and it will not be vulnerable to manipulation and adversarial inputs.

CONCLUSION

This research concludes with a complex analysis of the AI obstacles in banking industry impacting business data model enhancement. Both malicious AI use and adversarial attack are acknowledged, and yet Lack of Transparency and AI Model Theft has a higher impact on the corporate data model improvement. Banks must walk a tightrope between making sure their AI models are robust and yet transparent, provide ample IP protection and are secure. Future study of organizational culture and regulatory framework should be done to understand banking AI adoption challenges and drivers.

REFERENCES

- Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable AI (XAI). *IEEE Access*, *6*, 52138-5216.
- Anderson, R. (2021). *Artificial intelligence in banking: Risk management and compliance*. Financial Markets Journal, 36(4), 215-23. https://doi.org/1.1016/j.fmj.2021.01.004
- Arora, P., Gupta, R., & Singh, D. (2020). Legal challenges in AI and intellectual property protection. *Journal of Intellectual Property Law*, 22(1), 25-47.
- Binns, R. (2018). *Fairness in machine learning: Lessons from political philosophy*. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-14). ACM.
- Binns, R., Callaghan, V., & Wood, C. (2021). Ethical AI in banking: Protecting against malicious uses of AI. *Journal of Financial Regulation and Compliance*, 29(3), 225-238.
- Binns, R., Liu, Z., & Joshi, M. (2021). Protecting AI from malicious use in banking: A cybersecurity approach. *Journal of Banking Technology*, *29*(2), 113-128.
- Brown, G., & Grant, J. (2019). *AI and intellectual property theft in banking: Challenges and considerations*. Journal of Banking Technology, 33(2), 45-6.
- Brynjolfsson, E., & McAfee, A. (2017). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton & Company.
- Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). *Of, for, and by the people: The legal, ethical, and regulatory implications of autonomous driving*. *University of California Press*.
- Burrell, J. (2016). *How the machine 'thinks': Understanding opacity in machine learning algorithms*. Big Data & Society, 3(1), 1-19.
- Chen, X., Zhang, X., & Li, X. (2020). Data-driven AI models in banking: Enhancements in fraud detection and customer service. *International Journal of Bank Marketing, 38*(6), 1235-1256.
- Chesney, R., & Citron, D. K. (2019). *Deep fakes: A looming challenge for privacy, democracy, and national security*. *California Law Review*, 107(5), 1753-1819. https://doi.org/1.15779/Z38G37M76V
- Chui, M., & Manyika, J. (2020). *The potential for AI in banking and financial services*. McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/the-potential-for-ai-in-banking-and-financial-services

- Dastin, J. (2018). *Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
- Dastin, J., Shin, L., & Gray, C. (2022). The protection of AI models in banking: Intellectual property challenges. *Banking Innovation Journal*, *34*(3), 225-24.
- Dong, Z., Sun, L., & Xie, F. (2021). Defending digital banking from adversarial attacks: A security-focused AI approach. *Journal of Cybersecurity and Privacy*, 5(1), 33-5.
- Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., & Clement, M. (2021). *Artificial intelligence in banking and financial services: A review of applications, benefits, and challenges*. Journal of Financial Services Marketing, 26(2), 97-111. https://doi.org/1.1057/s41264-021-00101-9
- Fuster, A., & Greenfield, P. (2019). *AI model theft: A significant risk for financial institutions*. Journal of Cybersecurity, 5(3), 53-67. https://doi.org/1.1093/cybersecurity/tyz030
- Ghosh, D., & Choudhury, A. (2020). *AI in digital banking: Challenges and opportunities*. Journal of Banking & Finance, 44(8), 1905-1922. https://doi.org/1.1016/j.jbankfin.202.02.006
- Gilpin, L. H., Bau, D., Yuan, B. Z., Zhao, L., & Loper, M. (2018). *Explaining explanations: An overview of interpretability of machine learning*. In Proceedings of the 2018 ICML Workshop on Human Interpretability in Machine Learning (pp. 1-9).
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *Proceedings of the International Conference on Machine Learning*, 1-1.
- Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). *Explaining and harnessing adversarial examples*. In Proceedings of the International Conference on Machine Learning (ICML), 28(1), 1316-1324.
- Goodfellow, I., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. *International Conference on Machine Learning (ICML)*, 70, 1-9.
- Kshetri, N. (2020). *1 Artificial Intelligence in banking: Applications, challenges, and implications*. *Journal of Financial Technology*, 2(3), 45-63.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). *Deep learning*. Nature, 521(7553), 436-444. https://doi.org/1.1038/nature14539
- Lee, D. (2020). *Adversarial attacks on AI in banking systems: A study of risks and defenses*. AI & Ethics, 1(1), 23-34. https://doi.org/1.1007/s43681-020-00004-z
- Lipton, Z. C. (2018). The mythos of model interpretability. *Communications of the ACM*, 61(12), 36-43.
- Mansfield-Devine, S. (2020). AI-driven cybersecurity: New challenges for digital banking. *Network Security*, 2020(2), 12-19.
- Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2019). *A survey on bias and fairness in machine learning*. ACM Computing Surveys (CSUR), 54(6), 1-35. https://doi.org/1.1145/3285029

- O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.
- Papernot, N., McDaniel, P., & Goodfellow, I. J. (2016). *Transferability in machine learning: From phenomena to black-box attacks using adversarial samples*. In Proceedings of the 2016 IEEE European Symposium on Security and Privacy (pp. 1-16). IEEE.
- Papernot, N., McDaniel, P., & Goodfellow, I. J. (2017). *Practical black-box attacks against machine learning*. *Proceedings of the ACM on Computer and Communications Security*, 28(3), 1-17.
- Papernot, N., McDaniel, P., & Goodfellow, I. J. (2017). Towards deep learning security. *IEEE Transactions on Neural Networks and Learning Systems*, 28(4), 789-804.
- Patel, R. (2021). *The security risks of open-source AI in banking*. *Journal of Information Security*, 15(2), 100-11.
- Raji, I. D., & Buolamwini, J. (2019). *Actionable auditing: Investigating the impact of public policy on algorithmic fairness*. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-13.
- Raji, I. D., Buolamwini, J., & Gebru, T. (2020). Mitigating bias in AI models: Moving towards more transparent AI in banking. *AI & Ethics*, 2(2), 57-69.
- Zhang, Y., & Wu, X. (2021). *Data privacy and security concerns in AI-driven banking systems*. Journal of Financial Technology, 3(1), 19-29. https://doi.org/1.1016/j.jfintec.202.11.004