Journal of Islamic Monetary Economics and Finance, Vol. 12, No. 2 (2026), pp. 303 - 326
p-ISSN: 2460-6146, e-ISSN: 2460-6618

DOES CYBERSECURITY INFLUENCE THE IMPACT OF AI ON BANK RISK-TAKING? EVIDENCE FROM DUAL-BANKING COUNTRIES

Hasanul Banna[1,2*], Masagus M. Ridhwan[3,4] and Rudy Marhastari[3]

[1] Manchester Metropolitan University, United Kingdom; [2] Miyan Research Institute, International University of Business Agriculture and Technology, Bangladesh; [3] Bank Indonesia Institute, Bank Indonesia, Jakarta, Indonesia; [4] Perbanas Institute, Jakarta, Indonesia

ABSTRACT

Using 5,806 bank–year observations from 17 Asian and African economies over the years 2012–2022, we examine how artificial intelligence (AI) adoption influences bank risk-taking and whether cybersecurity capacity moderates this relationship. We find that AI intensity is associated with higher risk-taking at prevailing adoption levels. We also note that their relationship is concave, suggesting a shift from "risk-ramping" during early deployment to "discipline" as model governance and monitoring mature. We also find that stronger cybersecurity attenuates AI's marginal risk effect. Heterogeneity is evident: conventional banks exhibit higher turning points, reflecting a longer risk ramp, whereas Islamic banks peak earlier, consistent with stricter governance structures and more risk-averse practices. Results are robust in various sensitivity analyses. The findings suggest that AI scaling in banking requires synchronized advancement in cybersecurity and a model-risk management framework, aligned with evolving supervisory doctrine on digital resilience and AI governance.

Keywords: Artificial intelligence, Bank risk-taking, Cybersecurity, Islamic banking, Dual banking.
JEL classification: **G21; G28; G32; O33; C23**.

Article history:
Received : August 25, 2025
Revised : November 20, 2025
Accepted : May 22, 2026
Available online : June 30, 2026

https://doi.org/10.21098/jimf.v12i2.3476

* **CONTACT** Hasanul Banna: b.banna@mmu.ac.uk; Manchester Metropolitan University, Manchester M15 6BX, United Kingdom

I. INTRODUCTION

The integration of artificial intelligence (AI) into the banking sector has reached a critical juncture, revolutionising operational efficiency, credit underwriting, and real-time risk management. A Gartner study (2024) indicates that approximately 50 percent of banks have already incorporated AI into their operations, driven by capabilities such as fraud detection, algorithmic trading, and credit-scoring systems. However, as AI becomes increasingly integrated into financial decision-making processes, its interaction with cybersecurity frameworks assumes paramount importance.

AI's dual nature—serving both defensive and offensive purposes—adds complexity. On the one hand, AI enhances cybersecurity through threat intelligence automation, behavioural biometric anomaly detection, and predictive modelling. On the other side, these tools can be co-opted by cyber adversaries. Attackers are now deploying AI-enabled deepfakes, automated phishing campaigns, and malware capable of evading detection systems. Deloitte projects that AI-augmented fraud could cost the banking industry up to US$40 billion per year by 2027 while deepfake-initiated breaches have already caused substantial financial and reputational harm.

These dynamics escalate the stakes for risk-taking institutions. Major cybersecurity incidents—often originating from supply-chain vulnerabilities—are already disrupting continuity; in fact, over 80 % of cybersecurity leaders in North American banks contend that they cannot outpace AI-powered cybercriminals (Chan, 2025). Regulators have echoed these concerns: central banks and financial authorities worldwide are urging firms to implement zero-trust frameworks, AI-aware defence strategies, and enhanced vendor oversight (Times of India, 2025).

From a theoretical standpoint, AI's effect on risk-taking is non-linear: initial adoption may elevate risk due to model opacity and immature governance, while advanced adoption mitigates risk through embedded controls and learning effects—cybersecurity, in turn, moderates this trajectory by acting as a complementary capability that enables safe scaling of AI (Creese & Joshi, 2025).

In dual-banking systems—where conventional and Islamic banks coexist—the complexity intensifies as these banks operate under divergent regulatory regimes, risk appetites, and cybersecurity standards. Yet scant research has empirically examined how cybersecurity resilience moderates the relationship between AI adoption and risk-taking behaviours in such jurisdictions. Against this backdrop, our study asks: "Does cybersecurity influence the impact of AI on bank risk-taking in dual-banking countries?"

Although significant attention has been devoted to the potential of AI in the banking sector, empirical evidence on the impact of AI adoption on bank risk-taking behaviour remains limited, particularly across countries and in the context of cybersecurity. Bank risk-taking can manifest in diverse forms, such as default and leverage risk, and it is crucial to ascertain whether the adoption of AI technologies renders banks riskier or safer. Similarly, the influence of a bank's cybersecurity environment on its risk profile is not well understood, nor is it clear whether robust cybersecurity measures can mitigate the effects of AI on risk-taking. To address this knowledge gap, our study employs a panel dataset of banks spanning 17 countries from 2012 to 2022. The primary objective of this study

is to examine the impact of AI adoption on bank risk-taking and to investigate how cybersecurity factors affect this relationship.

Our paper presents several significant contributions. First, it introduces a novel cross-country measure of AI exposure and establishes a link between it and bank outcomes in dual-banking economies. Second, it provides the first systematic evidence of a non-linear (inverted-U) AI-risk-taking nexus, demonstrating that AI increases risk-taking behaviour at low-to-moderate adoption levels but becomes risk-reducing at higher levels of adoption. Third, it identifies cybersecurity as a moderator: the interaction between AI and cybersecurity is negative, indicating that stronger cyber capabilities mitigate AI's risk-taking effect. Fourthly, it uncovers bank-type heterogeneity, with Islamic banks exhibiting a significantly earlier turning point compared to conventional banks. This observation aligns with the notion that stricter governance and product constraints accelerate the transition to AI's risk-mitigating phase.

The remainder of the paper is organised as follows. The next section reviews relevant literature and develops our hypotheses. This is followed by the methodology section, which describes our data, variables, and empirical model. After that we provide the results of our analysis and discuss their implications. The final section offers concluding remarks and policy recommendations.

II. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1. AI Adoption and Bank Risk-Taking

Banks have rapidly adopted AI and data analytics to boost a wide range of functions. Particularly, AI adoption helps banks to process extensive datasets and differentiate patterns for improved decision-making. For instance, AI-driven systems ease risk management through more precise credit scoring, fraud detection, and loan monitoring (Sohail et al., 2021), which ultimately mitigate certain financial risks. Empirical evidence commences to support this perspective. Li et al. (2022) indicate that broader fintech adoption, encompassing AI, big data, and other related technologies, effectively diminishes Chinese banks' risk levels by enhancing operational efficiency and risk management practices. Similarly, a recent firm-level study finds that AI adoption tends to reduce overall financial risk by improving resource allocation and technological efficiency (Liu et al., 2025).

Nevertheless, there exists a compelling argument that AI can augment risk-taking, particularly during the initial stages of adoption or in the absence of robust governance frameworks. AI algorithms, particularly intricate machine learning models, can exhibit a "black box" phenomenon, in which their decisions are not always discernible, thereby complicating risk oversight. Model errors or biases inherent in AI systems could result in mispriced loans or strategic misjudgements that exacerbate credit and market risks. Notably, banks that have faced AI-related incidents, such as model failures or ethical lapses, exhibit bankruptcy risk and other adverse outcomes compared to those that have not experienced such incidents (Durongkadej et al., 2024). Industry experts warn that unrestricted AI usage may initiate operational and reputational risks. Mellen & Sharma (2024) suggest that organisations employing AI encounter concerns pertaining to lawsuits, bias, transparency, and cybersecurity threats emanating from AI applications. Recently,

Deloitte had to pay back USD 440,000 to the Australian government due to the misuse of AI (The Guardian, 2025). Furthermore, the FSB (2024) emphasises that AI could increase vulnerabilities such as third-party dependencies, correlated exposures, and cyber-attacks, thereby potentially increasing systemic risk if not appropriately managed. These perspectives collectively suggest that the net impact of AI on risk is ambiguous, potentially manifesting as a risk mitigator or a risk amplifier, contingent upon the manner in which it is employed.

One potential reconciliation of these divergent viewpoints is to consider non-linear effects. It is plausible that moderate adoption of AI may lead to increased risk-taking, while extensive and well-integrated adoption eventually reduces risk as the technology matures and risk-management benefits become evident. During early adoption phases, banks may employ AI aggressively to expand lending or trading activities, potentially outpacing their ability to fully comprehend or control the risks (an analogous "learning by doing" phase with heightened risk appetite). As AI usage becomes more sophisticated and pervasive, banks can harness it to bolster internal controls (e.g., real-time monitoring, advanced stress testing), thereby mitigating overall risk. This suggests an inverted U-shaped relationship between AI intensity and risk: risk-taking increases at low levels of AI adoption and diminishes at high levels of AI adoption. Such an inverted U pattern aligns with the notion that excessive use of a beneficial resource can reverse its impact—beyond a certain threshold, the incremental benefits of AI (particularly for risk management) surpass the initial risk-inducing effects. Based on this reasoning and the inconclusive evidence presented in prior literature, we propose our initial two hypotheses:

H1: Greater AI adoption by banks is associated with higher risk-taking.

In the lower range of AI intensity, banks that invest more in AI will exhibit higher default risk and leverage risk than those with less AI involvement (reflecting a risk-increasing effect of AI).

H2: The impact of AI on bank risk-taking is non-linear (inverted U-shaped).

That is, beyond a certain threshold, further increases in AI intensity will reduce bank risk-taking.

2.2. Interaction of AI and Cybersecurity

Cybersecurity is one of the important elements in maintaining financial stability in the digital age. Banks operate within a dynamic and adversarial cyber environment where threats such as hacking, malware, ransomware, and data breaches cause direct financial losses and erode customer trust. A major compromise of a major institution could potentially escalate into systemic problems. In response, regulatory authorities and international organisations have been actively promoting enhanced cyber resilience. The Global Cybersecurity Index (GCI) developed by the International Telecommunication Union (ITU) serves as a benchmark for countries based on their cybersecurity commitments across legal, technical, and organisational dimensions (ITU, 2024). While many countries, particularly financial centres, have strengthened their cyber defences and regulatory frameworks in recent years, global cyber capabilities remain uneven.

AI and cybersecurity are not mutually exclusive; in fact, they are increasingly interwoven within contemporary financial systems. AI, on one hand, can be employed to bolster cybersecurity measures. For instance, machine learning algorithms can detect anomalies and intrusions in real time, while AI-driven analytics can enhance fraud detection (Jada & Mayayise, 2024). Conversely, AI adoption itself can expand a bank's attack surface and introduce novel cyber vulnerabilities (Creese & Joshi, 2025). An automated decision engine or customer-facing chatbot of an AI system is a potential entry point that adversaries could exploit. This is mainly alarming if the AI relies on large data flows or external data sources that could be compromised through data poisoning or adversarial inputs. Subsequently, if a bank pursues AI innovation aggressively without appropriate attention to cybersecurity it may inadvertently increase its exposure to cyber risk. This suggests that the overall risk outcome of AI adoption could significantly depend on the cybersecurity context.

Scholars suggest an integrated approach to ensure that innovation does not outpace security controls (Creese & Joshi, 2025). They emphasise the need to embed cybersecurity at every stage of AI adoption. Organisations must assess and mitigate AI-related cyber risks, aligning AI deployments with a robust cyber risk management framework. When AI is implemented with strong security measures, such as secure data pipelines, access controls, and algorithmic transparency, the potential for AI-driven failures or attacks is significantly reduced (Jada & Mayayise, 2024). In such cases, AI's benefits, including efficiency, accuracy, and improved risk prediction, can be realised without a proportional increase in risk (AL-Dosari et al., 2024). Conversely, in environments with inadequate cybersecurity, AI adoption could exacerbate risks. Banks, for instance, may be vulnerable to cyberattacks exploiting their new digital tools or experience costly incidents due to a lack of oversight. Consequently, we posit that cybersecurity will mitigate the impact of AI on bank risk-taking. Specifically, a robust cybersecurity readiness will attenuate or negate the risk-enhancing effects of AI. Banks situated in jurisdictions with robust cybersecurity measures can adopt AI more safely, potentially even employing AI primarily for risk-mitigating applications. Conversely, banks in jurisdictions with inadequate cybersecurity frameworks may perceive AI as translating into heightened risk. The third hypothesis is:

H3: Cybersecurity moderates the impact of AI on risk-taking in a negative way.

The positive association between AI intensity and bank risk will be weaker (or reversed) when cybersecurity strength is high.

Together, these hypotheses set the stage for our empirical analysis. We next describe the data and methodology used to test H1–H3.

III. DATA AND METHODOLOGY

3.1. Data and Sample

To examine the influence of artificial intelligence (AI) and cybersecurity on bank risk taking, we construct a panel dataset of commercial banks spanning the period from 2012 to 2022. The sample comprises banks from 17 countries, predominantly in emerging and developing economies in Asia and Africa. These countries and their respective proportions within the sample are Bangladesh (11.07%), Indonesia

(18.02%), Malaysia (11.32%), Pakistan (8.47%), Thailand (6.34%), and several African nations, including Kenya (6.84%), Nigeria (4.89%), and South Africa (4.41%). The dataset comprises 5,806 bank-year observations. This extensive international sample enables us to capture the variability in both AI adoption and cybersecurity environments across diverse regulatory and market settings. The breakdown of the sample by country and by specification is in Appendix 1.

Our dataset is constructed by drawing upon multiple data sources. We obtain bank-level financial data from the Bureau van Dijk BankFocus database. We collect AI-related data from Crunchbase, cybersecurity data from the International Telecommunication Union (ITU), and macroeconomic variables from World Bank sources, including the World Development Indicators (WDI) and Worldwide Governance Indicators (WGI). Table 1 presents detailed descriptions of the variables and their descriptive statistics.

Table 1.
Descriptive Statistics

Variables	Definition	Obs	Mean	SD	Min	Max	Source
Dependent variables: Bank risk-taking							
DRISK	-1x [Log of Return on assets (ROA) plus Equity over total assets (EQT)divided by standard deviation of ROA (SDROA) using a 3-years rolling window of each bank]	5806	-3.863	1.249	-10.056	3.726	Bank Focus
LRISK	-1x [Log of (EQT/SDROA)]	5806	-3.783	1.257	-10.052	5.841	Bank Focus
Main independent variables							
AI Intensity	A country–year share of global AI firms	5806	0.085	0.059	0	0.241	Crunchbase
Cyber Security	The strength of a country's cybersecurity environment using the Global Cybersecurity Index (GCI)	4183	0.582	0.232	0.069	0.981	ITU
Bank-specific variables							
Bank Size	Log of total assets	5806	13.906	1.84	8.32	17.149	Bank Focus
Growth	Annual growth of total assets	5806	0.097	0.388	-0.897	17.202	Bank Focus
Deposit Share	Total deposits /total assets	5806	0.667	0.239	0	1.419	Bank Focus
Loan Share	Total Loans/total assets	5806	0.545	0.228	0	1.706	Bank Focus
Managerial Quality	Total earning assets/total assets	5806	0.804	0.166	0.007	1.003	Bank Focus
Macroeconomic variables							
GDP	Log of Annual Real GDP	5806	26.257	1.11	23.158	27.908	World Bank
Inflation	Annual Inflation	5806	4.673	3.319	0.674	13.246	World Bank
IQ	Institutional quality – Standardization using the Control of Corruption, Government Effectiveness, Political Stability and Absence of Violence/ Terrorism, Regulatory Quality, Rule of Law, and Voice and Accountability.	5806	-0.067	1.043	-2.148	1.747	World Bank

3.2. Empirical Model

3.2.1. Bank Risk-Taking

At the bank level, we focus on two indicators of risk-taking behaviour: default risk and leverage risk, as proposed by Danisman & Tarazi (2020) and Banna & Alam (2021). Default risk is proxied by the Z-score, which is calculated by dividing the return on assets (ROA) plus equity over total assets (EQT) by the standard deviation of ROA, using a 3-year rolling window for each bank. Leverage risk is proxied by EQT/σ (ROA). To simplify the analysis, we multiplied (-1) by the log(Z-score) to obtain DRISK and multiplied (-1) by the log of EQT/σ (ROA) to obtain LRISK. In our analysis, higher values of these risk measures correspond to greater risk-taking by the bank.

Although we refer to these measures as proxies for *bank risk-taking*, we acknowledge the conceptual distinction between "risk" and "risk-taking." In principle, risk-taking refers to banks' ex-ante behaviour, whereas risk reflects the ex-post realization of that behaviour in financial outcomes such as earnings volatility or insolvency likelihood. Following the established literature (e.g., Banna, 2025; Laeven & Levine, 2009; Čihák & Hesse, 2010; Bitar et al., 2020), we use ex post accounting-based indicators, such as the Z-score and leverage ratio, as observable outcomes of prior risk-taking decisions. Thus, our dependent variables capture the realized manifestation of banks' risk-taking behaviour over time, and we use the term "risk-taking outcomes" to maintain conceptual clarity.

3.2.2. Artificial Intelligence (AI)

Following the methodology of Abbasi et al. (2021) and Alam et al. (2025), AI adoption is quantified at the country level employing data sourced from Crunchbase. For each country and year, we determine the count of AI firms registered in Crunchbase and divide it by the global total of AI firms in that specific year. The resultant ratio (AI Intensity) encapsulates the country's proportion of global AI activity. This metric is subsequently mapped to all banks within the country for the corresponding year. The distribution exhibits significant variability, with a mean AI intensity of 0.085 (ranging from 0 to 0.241).

3.2.3. Cyber Security

Following Bruggemann et al. (2022), we proxy a nation's cybersecurity strength using the Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU). The GCI is a globally recognised composite index that evaluates each country's cybersecurity commitment across five pillars: legal measures, technical measures, organisational measures, capacity development, and international cooperation. The index is graded on a scale of 0 to 1, with higher values indicating enhanced cybersecurity preparedness and engagement.

3.2.4. Bank-Specific and Macro-Economic Variables

We also controlled for bank-specific and macroeconomic variables in our analysis. Following previous banking literature (e.g., Ahamed & Mallick, 2019; Banna & Alam, 2021), we consider the following variables as control variables.

For the bank-level variables, we use the logarithm of total assets (Bank size) to control the potential size effect of individual banks. We also use the ratio of total loans to total assets (Loan share) to account for the liquidity risk of individual banks. To control for deposit share, we use the ratio of total deposits to total assets (Deposit share). As better management quality can reduce excessive risk-taking, we consider the ratio of total earning assets to total assets (Management quality). We also control the annual growth of total assets (Growth).

For the country-level variables, we control for three macroeconomic variables: the log of annual real GDP (GDP), inflation, and the Good Governance/Institutional Quality (IQ) index, as published by the World Bank and Kaufmann et al. (2010). We use a standardised approach to measure institutional quality through the IQ index because these variables are highly correlated.

3.3. Empirical Methods

The following three regression models represent the relationship between AI and bank risk-taking and how cyber security moderates this relationship:

$$Y_{ijt} = \alpha + \beta AI_{jt} + \gamma B_{ijt} + \varphi M_{jt} + \varepsilon_{ijt} \quad (1)$$

$$Y_{ijt} = \alpha + \beta_1 (AI)_{jt} + \beta_2 (AI\ x\ AI)_{jt} + \gamma B_{ijt} + \varphi M_{jt} + \varepsilon_{ijt} \quad (2)$$

$$Y_{ijt} = \alpha + \beta_1 (AI)_{jt} + \beta_2 (AI\ x\ AI)_{jt} + \beta_3 (Cyber\ Security)_{jt} + \beta_4 (AI\ x\ Cyber\ Security)_{jt} + \gamma B_{ijt} + \varphi M_{jt} + \varepsilon_{ijt} \quad (3)$$

Y_{ijt} (i.e., DRISK or LRISK) is a proxy for the bank risk-taking of bank 'i' of country 'j' in year 't.' AI_{jt} = Artificial intelligence intensity of country 'j' in year 't.' $(AIxCyber\ Security)_{jt}$ = Interaction between AI and Cyber security of country 'j' in year 't.' B_{ijt} = bank-specific factors of bank 'i' of country 'j' in year 't'. M_{jt} = Macroeconomic factors of country 'j' in year 't.' β_1, β_2, γ, φ = Coefficients of the variables, and ε_{ijt} = Error term.

Regression (1) is our baseline specification, which is extended to capture non-linear relation between AI and risk taking in regression (2) and the moderating role of cybersecurity capacity on the relationship between AI intensity and bank risk-taking in regression (3). To ensure that the moderation effect is not confounded by the non-linear influence of AI, we re-estimated the model including both the linear and squared terms of AI intensity (AI and AI²) alongside their interaction with cybersecurity. The inclusion of these terms allows us to capture potential curvature effects in the presence of the moderator and mitigates the risk of omitted-variable bias (Wooldridge, 2010).

To ensure robustness, the study employs the High-Dimensional Fixed Effects estimation technique, with heteroscedasticity-corrected clustered robust standard errors to account for serial correlation and cross-sectional dependence. To address endogeneity concerns and sample selection bias, the study uses two-stage least squares (2SLS-IV) and Propensity Score Matching (PSM).

IV. RESULTS AND ANALYSIS

4.1. Results

Table 2 presents the Pearson pairwise correlation coefficients among all variables. The results indicate that no correlation coefficients are sufficiently high to suggest problematic multicollinearity, as all values are well below commonly used thresholds (i.e., $|r| < 0.80$). This suggests that the explanatory variables can be included together in the regression models without raising significant concerns regarding inflated standard errors or biased coefficient estimates.

Table 2.
Pairwise Correlations

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
(1) AI	1.000									
(2) Cyber Security	0.279*	1.000								
(3) Bank Size	0.165*	0.186*	1.000							
(4) Growth	-0.019	-0.051*	-0.014	1.000						
(5) Deposit Share	-0.082*	-0.124*	0.364*	0.017	1.000					
(6) Loan Share	0.086*	0.015	0.027	-0.051*	0.058*	1.000				
(7)Managerial Quality	0.209*	0.080*	0.256*	0.003	0.222*	0.484*	1.000			
(8) GDP	0.721*	0.406*	0.217*	0.006	-0.156*	0.100*	0.058*	1.000		
(9) Inflation	0.025	-0.260*	-0.126*	0.005	0.046*	-0.105*	-0.109*	-0.033	1.000	
(10) IQ	0.376*	0.387*	0.239*	-0.030	0.098*	0.155*	0.316*	0.111*	-0.589*	1.000

* shows significance at the .01 level

Table 3.
Baseline Regression (Full sample)

	Dependent variables			
	DRISK	LRISK	DRISK	LRISK
	(1)	(2)	(3)	(4)
AI	3.518***	3.306***	8.279***	8.393***
	(0.833)	(0.823)	(2.225)	(2.203)
AI x AI			-22.088**	-23.602***
			(9.239)	(9.111)
Bank Size	-0.160***	-0.133***	-0.162***	-0.136***
	(0.019)	(0.019)	(0.020)	(0.019)
Growth	0.156***	0.170***	0.156***	0.170***
	(0.053)	(0.057)	(0.053)	(0.058)
Deposit Share	0.673***	0.653***	0.659***	0.638***
	(0.148)	(0.156)	(0.147)	(0.155)
Loan Share	-0.321**	-0.349**	-0.316*	-0.344**
	(0.161)	(0.162)	(0.163)	(0.164)
Managerial Quality	-0.005	-0.027	-0.133	-0.164
	(0.215)	(0.223)	(0.226)	(0.234)

Table 3.
Baseline Regression (Full sample) Continued)

	Dependent variables			
	DRISK	**LRISK**	**DRISK**	**LRISK**
	(1)	**(2)**	**(3)**	**(4)**
GDP	-0.254***	-0.255***	-0.309***	-0.314***
	(0.044)	(0.045)	(0.052)	(0.051)
Inflation	0.032***	0.041***	0.029**	0.038***
	(0.012)	(0.012)	(0.012)	(0.012)
IQ	-0.049	-0.038	-0.051	-0.040
	(0.045)	(0.045)	(0.045)	(0.044)
Constant	4.287***	4.041***	5.727***	5.579***
	(1.127)	(1.130)	(1.318)	(1.315)
Year Fixed Effect	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes
Observations	5806	5806	5806	5806
R-squared	0.129	0.119	0.132	0.122
Adjusted R-squared	0.126	0.116	0.129	0.119
F Statistics	26.465***	23.772***	23.978***	21.590***

Standard errors are in parenthesis

*** p<0.01, ** p<0.05, * p<0.1

Table 3 shows the regression results for our two bank risk-taking measures: default risk and leverage risk. Across all specifications, we find strong support for our hypotheses. In Columns 1–2 present evidence that the coefficient on AI intensity exhibits a positive and statistically significant relationship with both risk measures (DRISK: 3.518; LRISK: 3.306), thereby supporting hypothesis H1. This suggests that banks located in countries with higher AI activity exhibit elevated default and leverage risk.

As for the controlled variables, we note that larger banks tend to exhibit lower risk (negative coefficient on size). Furthermore, faster asset growth and a higher deposit share are associated with increased risk, while a greater share of loans reduces risk, potentially indicating improved credit monitoring practices. Finally, higher inflation is correlated with increased risk, while higher real GDP is associated with reduced risk.

When the squared term of AI intensity is incorporated into the analysis (Columns 3–4), the linear term remains positive and exhibits a magnitude increase (DRISK: 8.279; LRISK: 8.393), while the squared term carries a negative and significant coefficient (DRISK: −22.088; LRISK: −23.602). These results unequivocally confirm hypothesis H2, indicating that the AI-risk relationship exhibits an inverted U-shape. In early AI adoption within banking, where implementation is moderate, risks increase proportionally due to operational complexity, immature processes, and integration challenges (Moharrak & Mogaji, 2024). AI systems may introduce vulnerabilities like bias and cyber risks without adequate safeguards. However, at advanced adoption stages, risks decrease as banks develop robust AI governance, monitoring systems, and expertise. Mature AI systems automate risk

management, enhance analytics, and strengthen compliance, reducing overall risk despite intensive deployment.

Calculating the turning point (−β_1/(2β_2)) yields AI intensity thresholds of approximately 0.187 for DRISK and 0.178 for LRISK. Given that the maximum AI intensity observed in our sample is 0.241, the majority of observations fall below the turning point, suggesting that the risk-increasing phase predominates. Nevertheless, banks situated in highly AI-intensive environments (top quantile) may still experience risk mitigation.

Table 4 presents the regressions separately for conventional and Islamic banks. While AI intensity exhibits a positive and substantial correlation with both types of banks, the coefficients exhibit significant disparities. For conventional banks, the linear AI term is 7.232 (DRISK) and 7.530 (LRISK), while the squared terms are −15.536 and −17.793. The turning point occurs at AI approximately equal to 0.233 for DRISK and 0.212 for LRISK, which is close to the maximum observed AI intensity. Consequently, conventional banks predominantly occupy the upward (risk-increasing) segment. In contrast, Islamic banks exhibit considerably larger linear coefficients (approximately 12.97 for DRISK and 12.79 for LRISK) and significantly more negative squared terms (approximately −72), resulting in turning points around AI approximately equal to 0.090. Given that the mean AI intensity (0.085) is close to this threshold, numerous Islamic banks are situated near or beyond the peak. This suggests that Islamic banks may transition to risk-reducing AI effects earlier than conventional banks. Shariah compliance inherently mandates risk-averse practices, such as the prohibition of excessive leverage, speculation, and certain high-risk financial instruments. Consequently, when Islamic banks integrate AI, they are less inclined to employ it in high-risk, speculative, or opaque applications (Ayedh et al., 2021).[1] This conservative approach may enable them to reach the inflection point of the inverted U-curve sooner, transitioning from risk-enhancing to risk-reducing effects of AI earlier than conventional banks.

Table 4.
Conventional vs Islamic Banks

	Dependent variables			
	Conventional Banks		**Islamic Banks**	
	DRISK	**LRISK**	**DRISK**	**LRISK**
	(1)	**(2)**	**(3)**	**(4)**
AI	7.232***	7.530***	12.972***	12.785***
	(2.725)	(2.695)	(3.169)	(3.182)
AI x AI	-15.536*	-17.793*	-72.227***	-72.257***
	(10.247)	(10.541)	(15.043)	(17.865)
Bank Size	-0.144***	-0.120***	-0.290***	-0.256***
	(0.020)	(0.020)	(0.068)	(0.066)
Growth	0.160***	0.178***	0.109	0.082
	(0.060)	(0.067)	(0.120)	(0.122)

1 In line with this finding, Law & Ridhwan (2022) also emphasize that the effect of Islamic financial system stability would positively enhance economic performance for the case of Indonesia.

Table 4.
Conventional vs Islamic Banks (Continued)

	Dependent variables			
	Conventional Banks		Islamic Banks	
	DRISK	LRISK	DRISK	LRISK
	(1)	(2)	(3)	(4)
Deposit Share	0.589***	0.549***	1.268***	1.411***
	(0.156)	(0.161)	(0.442)	(0.527)
Loan Share	-0.328*	-0.377**	0.167	0.215
	(0.174)	(0.174)	(0.473)	(0.501)
Managerial Quality	-0.151	-0.127	-0.547	-0.672
	(0.262)	(0.265)	(0.577)	(0.650)
GDP	-0.320***	-0.323***	-0.079	-0.090
	(0.058)	(0.058)	(0.159)	(0.170)
Inflation	0.018	0.024*	0.080***	0.089***
	(0.014)	(0.014)	(0.024)	(0.025)
IQ	-0.078	-0.068	0.096	0.089
	(0.053)	(0.052)	(0.076)	(0.075)
Constant	5.923***	5.736***	0.852	0.702
	(1.495)	(1.498)	(3.803)	(4.028)
Year Fixed Effect	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes
Observations	4984	4984	822	822
R-squared	0.119	0.108	0.285	0.273
Adjusted R-squared	0.115	0.104	0.267	0.255
F Statistics	17.612***	15.708***	16.246***	17.801***

Standard errors are in parenthesis

**** p<0.01, ** p<0.05, * p<0.1*

Table 5 reports the results on the moderating role of cybersecurity in the relationship between AI adoption and bank risk-taking. The interaction term between AI intensity and cybersecurity is negative and statistically significant in the full sample and for conventional banks across both risk proxies, consistent with Hypothesis H3. Specifically, the coefficients for AI × Cybersecurity are −2.994 (DRISK) and −2.834 (LRISK) for all banks and −3.434 (DRISK) and −3.204 (LRISK) for conventional banks. This indicates that stronger national cybersecurity environments reduce the marginal risk associated with AI. These findings imply that in high-cybersecurity jurisdictions AI adoption contributes less to risk-taking and may even become risk-mitigating at moderate intensity levels. Conversely, in countries with weaker cyber capabilities AI adoption is more strongly associated with risk escalation. This underscores the importance of cybersecurity as a complementary capability that conditions the risk trajectory of AI implementation.

Table 5.
The Impact of Cyber Security on AI-Bank Risk-Taking Nexus

	Dependent variables					
	All banks		Conventional Banks		Islamic Banks	
	DRISK	LRISK	DRISK	LRISK	DRISK	LRISK
	(1)	(2)	(3)	(4)	(5)	(6)
AI	8.374***	8.477***	6.901**	7.208***	12.606***	12.393***
	(2.218)	(2.198)	(2.711)	(2.687)	(3.234)	(3.221)
AI x AI	-14.892**	-16.808**	-6.095**	-9.002**	-74.773***	-75.249***
	(7.236)	(8.145)	(2.812)	(4.667)	(15.386)	(19.073)
Cyber Security	0.324***	0.316***	0.350***	0.341***	0.062	0.017
	(0.090)	(0.088)	(0.104)	(0.102)	(0.166)	(0.187)
AI x Cyber Security	-2.994***	-2.834***	-3.434***	-3.204***	1.378	1.456
	(0.785)	(0.767)	(0.894)	(0.874)	(1.618)	(1.614)
Bank Size	-0.165***	-0.139***	-0.147***	-0.123***	-0.289***	-0.255***
	(0.020)	(0.019)	(0.020)	(0.020)	(0.068)	(0.066)
Growth	0.154***	0.168***	0.157***	0.175***	0.123	0.093
	(0.053)	(0.058)	(0.060)	(0.066)	(0.128)	(0.131)
Deposit Share	0.648***	0.626***	0.582***	0.540***	1.217***	1.369**
	(0.149)	(0.156)	(0.158)	(0.163)	(0.457)	(0.550)
Loan Share	-0.310*	-0.339**	-0.314*	-0.363**	0.120	0.182
	(0.163)	(0.164)	(0.173)	(0.173)	(0.476)	(0.516)
Managerial Quality	-0.176	-0.206	-0.199	-0.175	-0.518	-0.640
	(0.225)	(0.233)	(0.262)	(0.264)	(0.581)	(0.654)
GDP	-0.315***	-0.320***	-0.318***	-0.321***	-0.085	-0.090
	(0.051)	(0.051)	(0.057)	(0.057)	(0.160)	(0.175)
Inflation	0.026**	0.036***	0.018	0.025*	0.084***	0.093***
	(0.012)	(0.012)	(0.014)	(0.014)	(0.026)	(0.026)
IQ	-0.062	-0.051	-0.083	-0.072	0.105	0.100
	(0.045)	(0.044)	(0.052)	(0.052)	(0.081)	(0.079)
Constant	5.890***	5.746***	5.859***	5.691***	1.003	0.697
	(1.300)	(1.298)	(1.470)	(1.475)	(3.819)	(4.161)
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5806	5806	4984	4984	822	822
R-squared	0.136	0.126	0.124	0.112	0.288	0.276
Adjusted R-squared	0.133	0.122	0.120	0.108	0.268	0.256
F Statistics	21.407***	19.221***	15.997***	14.121***	14.747***	16.745***

Standard errors are in parenthesis

*** *p<0.01, ** p<0.05, * p<0.1*

In contrast, the results for Islamic banks show that the AI × Cybersecurity interaction is positive but statistically insignificant for both DRISK and LRISK, suggesting no meaningful moderating effect. For Islamic banks, the smaller sample size (822 observations) may partly explain the statistically insignificant moderation effect of cybersecurity; hence, we interpret this result cautiously.

While AI intensity continues to exert a significant non-linear (inverted-U) influence on risk in Islamic banks—as evidenced by large and significant coefficients on both AI and AI^2—cybersecurity does not significantly alter this relationship. This likely reflects the more cautious and compliance-oriented adoption patterns of AI among Islamic banks (Abdullah et al., 2024). These institutions tend to deploy AI in low-risk domains such as internal efficiency, compliance, and reporting rather than in high-frequency trading, predictive credit scoring, or other data-intensive front-office functions, which are more exposed to cyber threats. Furthermore, the structure of Islamic banks, built around Shariah supervisory boards and guided by the Islamic Financial Services Board (IFSB), inherently promotes a more cautious approach. These Shariah boards add a unique layer of scrutiny, particularly when approving AI tools, ensuring they align with ethical and religious principles. This vetting process naturally directs banks away from high-risk or poorly understood algorithmic models. Furthermore, the IFSB's framework for risk and technology does not just encourage transparency and ethical use—it builds them into the system's foundation, effectively curbing AI's potential to amplify financial risk. Consequently, their exposure to AI-enabled cybersecurity vulnerabilities remains relatively limited, and the scope for cybersecurity to moderate the AI–risk nexus is correspondingly diminished.

4.2. Robustness Test

We conduct four robustness tests to substantiate that our baseline findings are not attributable to measurement choices, identification assumptions, or sample composition. First, we substitute AI intensity with ML intensity to ascertain whether the inverted-U relationship and the AI×Cyber moderation are not contingent upon a single proxy for digital capability (Shadish, Cook, & Campbell, 2002). Second, we use the standard deviation of ROA (SROA) as an alternative dependent variable. Third, we employ the 2SLS-IV estimation method employing AI_avg_year as instrument to mitigate endogeneity concerns arising particularly from reverse causality and omitted common shocks. This strengthens the causal interpretation of the concavity and interaction estimates (Angrist & Pischke, 2009; Imbens & Wooldridge, 2009). Lastly, the propensity score matching design is applied to arrive at matched sample higher- and lower-AI banks to minimise selection bias and model dependence, thereby confirming that results are not influenced by compositional differences in bank characteristics (Caliendo & Kopeinig, 2008). Consistency across these checks significantly enhances the credibility and external validity of our conclusions for both conventional and Islamic banks.

Table 6.
Robustness Test: Alternative AI Intensity (Machine Learning Intensity)

	Dependent variable: DRISK					
	All banks		Conventional Banks		Islamic Bank	
	(1)	(2)	(3)	(4)	(5)	(6)
ML	6.288***	6.211***	6.245***	5.749***	7.054***	6.794**
	(1.651)	(1.629)	(1.971)	(1.957)	(2.620)	(2.768)
ML x ML	-13.350***	-9.571**	-12.344**	-7.087**	-26.856***	-28.436***
	(4.393)	(4.488)	(5.126)	(3.364)	(5.737)	(5.529)
Cyber Security		0.246***		0.259***		0.105
		(0.076)		(0.088)		(0.156)
ML x Cyber Security		-2.194***		-2.531***		1.206
		(0.595)		(0.684)		(1.256)
Bank Size	-0.164***	-0.165***	-0.146***	-0.147***	-0.285***	-0.286***
	(0.020)	(0.019)	(0.020)	(0.020)	(0.067)	(0.066)
Growth	0.156***	0.151***	0.158***	0.152***	0.146	0.167
	(0.053)	(0.052)	(0.059)	(0.059)	(0.116)	(0.124)
Deposit Share	0.642***	0.620***	0.567***	0.548***	1.377***	1.323***
	(0.149)	(0.151)	(0.158)	(0.160)	(0.449)	(0.463)
Loan Share	-0.293*	-0.310*	-0.307*	-0.323*	0.364	0.318
	(0.163)	(0.163)	(0.175)	(0.174)	(0.478)	(0.481)
Managerial Quality	0.012	-0.019	-0.038	-0.079	-0.531	-0.514
	(0.212)	(0.212)	(0.254)	(0.254)	(0.570)	(0.568)
GDP	-0.276***	-0.272***	-0.294***	-0.280***	-0.129	-0.142
	(0.049)	(0.049)	(0.054)	(0.054)	(0.156)	(0.161)
Inflation	0.036***	0.035***	0.026**	0.028**	0.066***	0.069***
	(0.011)	(0.011)	(0.013)	(0.013)	(0.024)	(0.025)
IQ	-0.058	-0.056	-0.085	-0.075	0.050	0.053
	(0.047)	(0.046)	(0.054)	(0.054)	(0.085)	(0.087)
Constant	4.833***	4.766***	5.232***	4.898***	1.978	2.313
	(1.252)	(1.242)	(1.390)	(1.382)	(3.737)	(3.866)
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5806	5806	4984	4984	822	822
R-squared	0.130	0.133	0.118	0.122	0.280	0.285
Adjusted R-squared	0.127	0.130	0.114	0.118	0.262	0.265
F Statistics	23.383***	21.175***	17.274***	16.135***	15.046***	13.678***

Standard errors are in parenthesis
*** *p<0.01*, ** *p<0.05*, * *p<0.1*

In Table 6, we employ Machine Learning (ML) Intensity (country-year share of global ML firms) as an alternative proxy for AI intensity. The outcomes align with the baseline findings. These results also help to mitigate concerns that our primary AI intensity proxy may be sensitive to country size. The consistency of coefficients when using Machine Learning (ML) Intensity supports the robustness and scalability of our measurement approach across economies of different scales.

Table 7.
Robustness Test: Alternative Risk-Taking

	Dependent variable: SROA					
	All banks		Conventional Banks		Islamic Bank	
	(1)	(2)	(3)	(4)	(5)	(6)
AI	0.062***	0.062***	0.082***	0.082***	0.088	0.066
	(0.015)	(0.015)	(0.015)	(0.016)	(0.062)	(0.062)
AI x AI	-0.251***	-0.247***	-0.296***	-0.275***	-0.558*	-0.756**
	(0.065)	(0.068)	(0.063)	(0.067)	(0.325)	(0.334)
Cyber Security		0.002**		0.003**		-0.004
		(0.001)		(0.001)		(0.003)
AI x Cyber Security		-0.002**		-0.007**		0.081**
		(0.001)		(0.003)		(0.032)
Bank Size	-0.003***	-0.003***	-0.002***	-0.002***	-0.003***	-0.003***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
Growth	0.001**	0.001**	0.002***	0.002***	0.001	0.001
	(0.001)	(0.001)	(0.000)	(0.000)	(0.002)	(0.002)
Deposit Share	-0.011***	-0.011***	-0.010***	-0.010***	-0.026***	-0.027***
	(0.001)	(0.001)	(0.001)	(0.001)	(0.005)	(0.005)
Loan Share	-0.005***	-0.005***	-0.005***	-0.005***	-0.022***	-0.022***
	(0.001)	(0.001)	(0.001)	(0.001)	(0.005)	(0.005)
Managerial Quality	-0.003*	-0.003*	-0.005***	-0.006***	0.028***	0.030***
	(0.002)	(0.002)	(0.002)	(0.002)	(0.006)	(0.006)
GDP	-0.002***	-0.002***	-0.002***	-0.002***	-0.004***	-0.003**
	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
Inflation	0.000***	0.000***	0.000	0.000	0.002***	0.002***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
IQ	0.001**	0.001**	-0.000	-0.000	0.004***	0.005***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.001)	(0.001)
Constant	0.097***	0.097***	0.098***	0.097***	0.164***	0.147***
	(0.009)	(0.009)	(0.008)	(0.008)	(0.037)	(0.038)
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5806	5806	4984	4984	822	822
R-squared	0.169	0.169	0.184	0.184	0.228	0.235
Adjusted R-squared	0.166	0.166	0.180	0.180	0.209	0.214
F Statistics	114.293***	95.217***	108.753***	90.725***	21.130***	18.344***

Standard errors are in parenthesis
*** p<0.01, ** p<0.05, * p<0.1

In Table 7, we re-estimated the models using the standard deviation of ROA as an alternative risk-taking measure, which again produce results consistent with those based on Z-score and leverage risk.

Table 8.
Robustness Test: 2SLS-IV (Endogeneity Issue)

	Dependent variable: DRISK					
	All banks		Conventional Banks		Islamic Bank	
	(1)	(2)	(3)	(4)	(5)	(6)
AI	11.853***	11.212***	10.064***	8.836***	21.893***	19.926***
	(2.573)	(2.534)	(2.970)	(2.936)	(5.726)	(5.475)
AI x AI	-39.694***	-30.164***	-31.770***	-17.372**	-92.738***	-97.308***
	(10.282)	(10.206)	(11.794)	(7.871)	(25.372)	(25.061)
Cyber Security		0.248***		0.317***		0.031
		(0.075)		(0.089)		(0.139)
AI x Cyber Security		-2.222***		-3.071***		1.471
		(0.682)		(0.791)		(1.433)
Bank Size	-0.175***	-0.177***	-0.161***	-0.163***	-0.266***	-0.264***
	(0.022)	(0.022)	(0.022)	(0.022)	(0.082)	(0.083)
Growth	0.157***	0.155***	0.157**	0.153**	0.196*	0.191*
	(0.057)	(0.057)	(0.064)	(0.063)	(0.105)	(0.109)
Deposit Share	0.948***	0.942***	0.887***	0.881***	1.381***	1.342**
	(0.149)	(0.149)	(0.160)	(0.160)	(0.535)	(0.536)
Loan Share	-0.180	-0.174	-0.212	-0.198	0.158	0.156
	(0.161)	(0.161)	(0.172)	(0.171)	(0.512)	(0.507)
Managerial Quality	-0.432**	-0.429**	-0.369	-0.361	-1.000*	-0.944*
	(0.205)	(0.204)	(0.237)	(0.235)	(0.528)	(0.525)
GDP	-0.340***	-0.341***	-0.323***	-0.321***	-0.460**	-0.332*
	(0.065)	(0.063)	(0.067)	(0.065)	(0.213)	(0.196)
Inflation	0.002	0.000	-0.001	-0.001	0.007	0.026
	(0.011)	(0.011)	(0.012)	(0.012)	(0.029)	(0.030)
IQ	-0.073*	-0.087**	-0.078	-0.096**	-0.071	-0.021
	(0.043)	(0.042)	(0.049)	(0.048)	(0.100)	(0.094)
Constant	6.266***	6.276***	5.735***	5.632***	10.231*	6.843
	(1.635)	(1.600)	(1.689)	(1.644)	(5.482)	(5.119)
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5806	5806	4984	4984	822	822
R-squared	0.124	0.129	0.112	0.118	0.248	0.265
Chi-sq	246.952***	262.444***	199.425***	225.373***	116.508***	118.924***

Standard errors are in parenthesis
*** *p<0.01, ** p<0.05, * p<0.1*

Table 8 presents results from a two-stage least squares (2SLS) instrumental variable approach to address potential endogeneity concerns—particularly reverse causality and omitted variable bias. We instrument AI intensity using AI_avg_year, defined as the annual average of AI intensity across all countries in the sample. This variable captures exogenous time-series variation in global AI activity, which influences country-level AI diffusion but is plausibly unrelated to idiosyncratic bank-level risk shocks. The 2SLS results yield larger positive linear coefficients

and stronger negative coefficients of the quadratic terms, reaffirming the inverted U-shaped relationship. Importantly, the AI × Cybersecurity interaction remains negative and significant for conventional banks, reinforcing the moderation effect while accounting for potential endogeneity. As an additional robustness check, we also employ lagged AI intensity (AI_{t−1}) as an alternative instrument for current AI adoption. The estimates remain consistent with those obtained using the AI_avg_year instrument, further supporting the robustness of our results against potential simultaneity bias.

Table 9.
Robustness Test: Propensity Score Matching (PSM)

	Dependent variable: DRISK					
	All banks		Conventional Banks		Islamic Bank	
	(1)	(2)	(3)	(4)	(5)	(6)
AI	7.776***	7.939***	6.582**	6.474**	13.017***	12.644***
	(2.223)	(2.225)	(2.721)	(2.716)	(3.167)	(3.240)
AI x AI	-22.091**	-16.738**	-15.083**	-7.944**	-72.502***	-75.117***
	(9.252)	(8.238)	(7.725)	(3.812)	(15.044)	(15.441)
Cyber Security		0.232***		0.253**		0.058
		(0.089)		(0.105)		(0.171)
AI x Cyber Security		-2.221***		-2.624***		1.399
		(0.787)		(0.914)		(1.648)
Bank Size	-0.160***	-0.163***	-0.143***	-0.146***	-0.289***	-0.288***
	(0.020)	(0.020)	(0.020)	(0.020)	(0.068)	(0.068)
Growth	0.158***	0.157***	0.162***	0.160***	0.106	0.120
	(0.055)	(0.055)	(0.062)	(0.062)	(0.121)	(0.129)
Deposit Share	0.608***	0.609***	0.537***	0.543***	1.262***	1.211***
	(0.147)	(0.148)	(0.156)	(0.157)	(0.444)	(0.458)
Loan Share	-0.303*	-0.296*	-0.327*	-0.310*	0.172	0.126
	(0.165)	(0.165)	(0.177)	(0.176)	(0.473)	(0.477)
Managerial Quality	-0.163	-0.190	-0.163	-0.197	-0.560	-0.530
	(0.226)	(0.226)	(0.263)	(0.263)	(0.580)	(0.583)
GDP	-0.261***	-0.275***	-0.269***	-0.278***	-0.078	-0.083
	(0.052)	(0.052)	(0.059)	(0.058)	(0.162)	(0.164)
Inflation	0.039***	0.035***	0.028**	0.027*	0.080***	0.084***
	(0.012)	(0.012)	(0.014)	(0.014)	(0.025)	(0.027)
IQ	-0.028	-0.041	-0.054	-0.063	0.098	0.107
	(0.044)	(0.045)	(0.052)	(0.052)	(0.076)	(0.081)
Constant	4.477***	4.829***	4.600***	4.830***	0.820	0.951
	(1.326)	(1.334)	(1.511)	(1.508)	(3.920)	(3.969)
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Bank Clustered	Yes	Yes	Yes	Yes	Yes	Yes
SE Clustered	Yes	Yes	Yes	Yes	Yes	Yes
Observations	5704	5704	4885	4885	819	819
R-squared	0.125	0.127	0.110	0.112	0.284	0.288
Adjusted R-squared	0.122	0.124	0.106	0.108	0.266	0.268
F Statistics	22.582***	19.802***	15.999***	14.228***	16.186***	14.664***

Standard errors are in parenthesis
*** p<0.01, ** p<0.05, * p<0.1

Furthermore, in Table 9, we apply a propensity score matching (PSM) technique to further address potential sample selection bias by following recent banking literature (e.g., Elnahass et al., 2021). Given that AI intensity is a country-level variable while our outcomes are measured at the bank level, we define treatment status as banks operating in countries with AI intensity above the cross-sectional mean. Propensity scores are estimated using observable bank-level and macroeconomic covariates that may jointly influence both AI exposure and risk-taking. Treated and control banks are then matched using 1:1 nearest-neighbour matching without replacement. This procedure ensures comparability between banks in high- and low-AI-intensity environments, holding observable characteristics constant. The matched-sample results replicate the baseline findings, with statistically significant AI and AI^2 effects and a consistently negative AI × Cybersecurity interaction for all and conventional banks, thereby strengthening the robustness of our main conclusions.

We summarize the robustness outcomes in Table 10. Across all alternative specifications, the inverted U-shaped AI–risk relationship and the moderating role of cybersecurity remain consistent, underscoring the robustness of our findings.

Table 10.
Robustness Summary Table

Robustness Test	Purpose	Key Finding
Alternative AI Proxy (ML Intensity)	Checks construct validity	Inverted U-shape and AI×Cyber moderation remain significant
Alternative Risk Measure (SROA)	Validates risk proxy robustness	Results unchanged
2SLS-IV	Addresses endogeneity	Similar sign and significance
Propensity Score Matching (PSM)	Controls for sample-selection bias	Consistent with baseline

V. CONCLUSION AND RECOMMENDATIONS

5.1. Conclusion

This paper presents comprehensive, cross-country, and bank-level evidence demonstrating a statistically and economically significant correlation between AI adoption and a rise in bank risk-taking at low to moderate levels of adoption. Subsequently, there appears to be a period of discipline as AI adoption increases further. This pattern is consistent with the co-evolution of monitoring, validation, and governance capabilities. Specifically, the linear term for AI is positively significant for both default and leverage risk. Conversely, the squared term is negatively significant in baseline and subsample regressions. The effect is more pronounced and persistent for conventional banks compared to Islamic banks, which exhibit earlier peaks in the AI-risk profile. Furthermore, national cybersecurity capacity significantly reduces the risk-raising margin of AI. The AI×Cyber term is negatively significant in both the full and conventional-bank samples, indicating that stronger cyber environments mitigate AI-induced risk-taking. However, this interaction is relatively small and imprecise for Islamic banks at their current adoption levels. These findings are robust in various sensitivity tests.

These findings align with the prevailing supervisory doctrine. Recent revisions to the Basel Core Principles enhance expectations for operational resilience and digitalisation risk; the Financial Stability Board (FSB) emphasises monitoring deficiencies and correlated exposures stemming from prevalent AI models and third-party dependencies; and the Prudential Regulation Authority (PRA) encapsulates governance, validation, and mitigants for intricate (including AI/ML) models. Collectively, these frameworks precisely anticipate the channels through which our estimates function: early-phase AI facilitates the expansion of origination and decision velocity, thereby augmenting risk-taking; meanwhile, maturing controls and cyber capabilities effectively restrain risk and mitigate AI's marginal impact.

5.2. Policy Recommendations

The results of this study suggest that AI adoption has a non-linear impact on bank risk-taking, initially amplifying risk before stabilizing as governance and cybersecurity maturity increase. Accordingly, policy interventions should aim to manage this "risk-ramp" through stronger governance, cyber readiness, and coordinated supervision across institutions.

Banks should adopt stage-gated AI rollouts with conservative limits, post-model overlays, challenger testing, and live drift monitoring until validation and governance frameworks demonstrate sustained effectiveness. In parallel, banks should strengthen data governance and model transparency frameworks, ensuring traceable data provenance, explainable AI outputs, and secure storage of training data to comply with emerging AI accountability standards. Early adoption should be treated as risk-amplifying by default, with cybersecurity uplift made a precondition for scaling high-impact AI use cases. This includes tightening identity and access controls, maintaining a consistent patch cadence, establishing data lineages, and developing robust incident response plans. Differentiate based on model is needed: conventional banks should anticipate a longer "risk-ramp" and maintain stricter overlays in retail and SME credit, as well as treasury operations. Islamic banks should integrate Shariah-aware MRM frameworks (labelled datasets, explainability to Shariah committees) due to earlier turning points and reputational risk channels.

Central banks should conduct an annual sector-wide AI–Cyber supervisory stress test that mandates bank-level AI model inventories, vendor concentration maps, and auditable cyber performance metrics (e.g., Mean Time to Down (MTTD) and Mean Time to Repair (MTTR), critical patch latency). Outcomes should be linked to proportionate Pillar-2 scalars or growth constraints until remediation is validated. Over time, supervisory stress-test outcomes could be linked to cyber-resilience buffers or capital planning adjustments, aligning cybersecurity readiness with prudential expectations. Common data standards should be established for model taxonomy, materiality tiers, and incident reporting (including Islamic-specific tags). Systemic surveillance should be expanded to monitor homogeneity in models and cloud providers that can transmit common shocks.

Regulators should establish comprehensive AI-inclusive model risk management frameworks by integrating existing local regulations and ensuring

compliance through SREP/Pillar-2 outcomes. This includes strengthening technology-risk and third-party oversight (secure MLOps pipelines, adversarial testing for high-materiality AI, registers of critical ICT providers) to facilitate AI scaling in tandem with operational resilience. Both regulators and central banks should also invest in technical capacity building, including AI model audit training, cyber-forensics expertise, and supervisory data analytics, to ensure oversight keeps pace with innovation. Such measures will facilitate AI scaling in tandem with operational resilience and cybersecurity safeguards.

Overall, a coordinated approach among regulators, central banks, and financial institutions is essential to ensure that AI-driven innovation enhances financial stability rather than undermines it. Given the cross-border nature of AI supply chains and cyber vulnerabilities, international cooperation among supervisory authorities will be vital to prevent contagion effects from common technological shocks. Building strong cybersecurity capabilities and clear AI governance frameworks at all levels will help the financial sector harness the benefits of AI while minimizing its risks.

5.3. Limitations and Future Research

Our study has several limitations, which suggest areas for future research. First, we consider country-level AI intensity and cybersecurity measures. Future research could utilise firm-level data such as AI expenditure, disclosures, patents, and job postings, as well as cybersecurity reports, incidents, and policies. Second, we have considered only default and leverage risk. Future research could include market, operational, reputational, and other non-traditional risks. Finally, our study period spans from 2012 to 2022; however, future research can be extended to 2025.

REFERENCES

Abbasi, K., Alam, A., Brohi, N. A., Brohi, I. A., & Nasim, S. (2021). P2P lending Fintechs and SMEs' access to finance. *Economics Letters*, *204*, 109890.

Abdullah, O., Shaharuddin, A., Wahid, M. A., & Harun, M. S. (2024). AI applications for fiqh rulings in Islamic Banks: Shariah committee acceptance. *ISRA International Journal of Islamic Finance*, *16*(1), 111-126.

Ahamed, M. M., & Mallick, S. K. (2019). Is financial inclusion good for bank stability? International evidence. *Journal of Economic Behavior & Organization*, *157*, 403-427.

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and Systems*, *55*(2), 302-330.

Alam, A., Banna, H., Roni, N. N., & Abedin, M. Z. (2025). Sowing Sustainability: How does fintech mitigate agricultural financial risk from climate change vulnerability. *International Review of Economics & Finance*, *101*, 104226.

Angrist, J. D., & Pischke, J. S. (2009). *Mostly harmless econometrics: An empiricist's companion*. Princeton, New Jersey: Princeton University Press.

Ayedh, A. M., Mahyudin, W. A. T., Abdul Samat, M. S., & Muhamad Isa, H. H. (2021). The integration of Shariah compliance in information system of Islamic

financial institutions: Qualitative evidence of Malaysia. *Qualitative Research in Financial Markets*, *13*(1), 37-49.

Banna, H. (2025). Digital financial inclusion and bank stability in a dual banking system: Does financial literacy matter?. *Journal of Islamic Monetary Economics and Finance*, *11*(1), 63-90.

Banna, H., & Alam, M. R. (2021). Does digital financial inclusion matter for bank risk-taking? Evidence from the dual-banking system. *Journal of Islamic Monetary Economics and Finance*, *7*(2), 401-430.

Bitar, M., Pukthuanthong, K., & Walker, T. (2020). Efficiency in Islamic vs. conventional banking: The role of capital and liquidity. *Global Finance Journal*, *46*, 100487.

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, *159*(1), 125-143.

Caliendo, M., & Kopeinig, S. (2008). Some practical guidance for the implementation of propensity score matching. *Journal of Economic Surveys*, *22*(1), 31-72.

Chan, B. (2025). Wall Street is worried it can't keep up with AI-powered cybercriminals. Retrieved from https://www.businessinsider.com/banks-ai-cybersecurity-threats-hackers-generative-ai-2025-3

Čihák, M., & Hesse, H. (2010). Islamic banks and financial stability: An empirical analysis. *Journal of Financial Services Research*, *38*(2), 95-113.

Creese, S. & Joshi, A. (2025). Securing innovation: A leader's guide to managing cyber risks from AI adoption. Retrieved from https://www.weforum.org/stories/2025/01/a-leaders-guide-to-managing-cyber-risks-from-ai-adoption/

Danisman, G. O., & Tarazi, A. (2020). Financial inclusion and bank stability: Evidence from Europe. *The European Journal of Finance*, *26*(18), 1842-1855.

Durongkadej, I., Hu, W., & Wang, H. E. (2024). How artificial intelligence incidents affect banks and financial services firms? A study of five firms. *Finance Research Letters*, *70*, 106279.

Elnahass, M., Trinh, V. Q., & Li, T. (2021). Global banking stability in the shadow of Covid-19 outbreak. *Journal of International Financial Markets, Institutions and Money*, *72*, 101322.

Financial Stability Board (FSB). (2024). The financial stability implications of artificial intelligence. Retrieved from https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence

Gartner. (2024). *2025 Gartner CIO and Technology Executive survey*. Gartner, Inc. Retrieved from https://www.gartner.com/en/documents/5848147

Imbens, G. W., & Wooldridge, J. M. (2009). Recent developments in the econometrics of program evaluation. *Journal of Economic Literature*, *47*(1), 5-86.

International Telecommunication Union (ITU). (2024). Global Cybersecurity Index (5th ed.). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2), 100063.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2010). The worldwide governance indicators: A summary of methodology. *Data and Analytical Issues, World Bank Policy Research Working Paper, 5430*.

Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of Financial Economics*, *93*(2), 259-275.

Law, S. H., & Ridhwan, M. M. (2022). Effect of Islamic financial system stability on economic performance in Indonesia. *Journal of Islamic Monetary Economics and Finance*, *8*(3), 371-406.

Li, G., Elahi, E., & Zhao, L. (2022). Fintech, bank risk-taking, and risk-warning for commercial banks in the era of digital technology. *Frontiers in Psychology*, *13*, 934053.

Liu, Y., Abdul Rahman, A., Imna Mohd Amin, S., & Ja'afar, R. (2025). Navigating fintech and banking risks: Insights from a systematic literature review. *Humanities and Social Sciences Communications*, *12*(1), 1-16.

Mellen, D. & Sharma, V. (2024). Why CISOs must cultivate a cyber-secure workforce in the age of AI. Retrieved from https://www.ey.com/en_uk/insights/consulting/why-cisos-must-cultivate-a-cyber-secure-workforce-in-the-age-of-ai

Moharrak, M., & Mogaji, E. (2025). Generative AI in banking: Empirical insights on integration, challenges and opportunities in a regulated industry. *International Journal of Bank Marketing*, *43*(4), 871-896.

Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston: Houghton Mifflin.

Sohail, O., Sharma, P., Sidhu, S., et al. (2021). The future of AI in banking. Retrieved from https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/consulting/2024/us-ai-transforming-future-of-banking.pdf

The Guardian. (2025). *Deloitte to pay money back to Albanese government after using AI in $440,000 report.* Retrieved from https://www.theguardian.com/australia-news/2025/oct/06/deloitte-to-pay-money-back-to-albanese-government-after-using-ai-in-440000-report

Times of India. (2025). *Cyber risks in financial sector RBI calls for AI aware defence and zero trust approach warns of systemic threat from vendor lock-ins.* Retrieved from https://timesofindia.indiatimes.com/business/cybersecurity/cyber-risks-in-financial-sector-rbi-calls-for-ai-aware-defence-and-zero-trust-approach-warns-of-systemic-threat-from-vendor-lock-ins/articleshow/122164857.cms

Wooldridge, J. M. (2010). *Econometric analysis of cross section and panel data* (2nd ed.). London: MIT Press.

APPENDIX

Appendix 1.
The Breakdown of the Sample by Country by Specification

Country	All banks observations	Conventional banks observations	Islamic banks observations
Bangladesh	643	564	79
Benin	70	68	2
Indonesia	1,046	953	93
Iraq	271	180	91
Jordan	244	196	48
Kenya	397	381	16
Malaysia	657	461	196
Nigeria	284	281	3
Pakistan	492	428	64
Philippines	292	286	6
Qatar	110	65	45
Senegal	175	168	7
Seychelles	56	54	2
South Africa	256	245	11
Sudan	163	16	147
Thailand	368	364	4
United Republic of Tanzania	282	274	8
Total observation-year	5806	4984	822