



INTEGRATING FINTECH, AI, AND CYBERSECURITY IN ISLAMIC BANKING: A SHARIAH-COMPLIANT FRAMEWORK FOR INNOVATION AND RISK MANAGEMENT

**Zahiduzzaman Zahid^{1*}, Md. Shahed Alamm², Munshi Md Ashfaul Alam³, Md.
Syful Islam⁴, Md. Mozammel Hoque⁵**

drzahid.mailbox@gmail.com¹, shahedssdu@gmail.com², mmashfaul@gmail.com³,
msyful@yahoo.com⁴, mmhoque2018@gmail.com⁵

**^{1*}University of the Cumberlands, Williamsburg, Kentucky, United States of
America**

²Islamic Financing Division, Bangladesh Finance PLC, Dhaka, Bangladesh

**³Islamic Financing Wing & Strategic Recovery Unit, Bangladesh Finance PLC,
Dhaka, Bangladesh**

⁴Pubali Bank PLC, Dhaka, Bangladesh

⁵Sammilito Islami Bank PLC, Dhaka, Bangladesh

Abstract,

This study examines how Financial Technology (FinTech), Artificial Intelligence (AI), and cybersecurity are being integrated into Islamic banking without compromising Shariah principles. Established adoption models explain behavioural intention well but remain religion-neutral, and therefore overlook the ethical conditions that govern Islamic financial institutions (IFIs). The study develops the Shariah-Tech Adoption Framework (STAF), which extends the Technology Acceptance Model and Innovation Diffusion Theory with Shariah Compliance Theory and Cybersecurity Risk Management Theory, and introduces Perceived Shariah Compatibility (PSC) as a moderating construct. A mixed-methods design was applied, combining a structured survey of 150 Islamic finance professionals across the Gulf Cooperation Council (GCC) and Southeast Asia, twenty semi-structured interviews, and three institutional case studies drawn from Bank Al Jazira, Dubai Islamic Bank, and Al Rajhi Bank. PSC significantly predicts adoption intention, and adopting institutions report faster processing, wider financial inclusion, and lower fraud exposure. Cultural resistance, a shortage of combined AI and Shariah expertise, and regulatory ambiguity remain the principal barriers. The study contributes a testable, context-specific adoption framework and offers policy directions on ethical AI governance, zero-trust cybersecurity, and regulatory harmonisation for IFIs pursuing digital transformation.

Keywords: Islamic FinTech, Artificial Intelligence, Shariah Compliance

INTRODUCTION

Financial services have been reshaped over the past decade by the convergence of Financial Technology (FinTech), Artificial Intelligence (AI), and cybersecurity. Mobile banking platforms, distributed ledgers, and predictive analytics have altered how transactions are initiated, priced, monitored, and secured. The effects extend beyond convenience: digital rails have lowered the cost of reaching underserved populations, machine learning has improved the accuracy

15

**Zahiduzzaman Zahid, Md. Shahed Alamm, Munshi Md Ashfaul Alam, Md. Syful Islam,
Md. Mozammel Hoque**

<http://jurnal.iain-padangsidimpuan.ac.id/index.php/jiftech>



of credit and fraud decisions, and layered security architectures have become a precondition for institutional trust. For banks of every orientation, technology is no longer a support function but a determinant of competitiveness and resilience.

Islamic banking approaches this transition from a distinctive position. Its operations are bounded by Shariah, which prohibits *riba* (interest), *maysir* (speculation), and *gharar* (excessive uncertainty), and which excludes financing of haram sectors such as alcohol, gambling, and conventional armaments. In place of interest-bearing intermediation, Islamic finance relies on risk-sharing and asset-backed structures such as *mudarabah*, *musharakah*, *murabahah*, and *sukuk*, and is oriented towards the *Maqasid al-Shariah*, the higher objectives concerning the preservation of religion, life, intellect, progeny, and wealth (Chapra, 2008). Technology adoption in this setting is therefore not only a question of efficiency and usability; every innovation must also be assessed for its compatibility with an ethical and legal order that operates prior to, and independently of, commercial logic.

The industry within which this question arises is substantial and still expanding. S&P Global Ratings (2025) reports that the global Islamic finance industry grew by 10.6 per cent in 2024, driven by the expansion of Islamic banking assets and by *sukuk* issuance, with total *sukuk* outstanding surpassing one trillion United States dollars for the first time. Continued positive growth was expected through 2025, although the outlook is qualified by oil price sensitivity and by the possible adoption of Shariah Standard 62, which could reclassify *sukuk* from debt-like to equity-like instruments. Alongside this, Islamic FinTech has developed into a distinct segment with its own market structure, concentrated in Saudi Arabia, Malaysia, Indonesia, the United Arab Emirates, and the United Kingdom (DinarStandard & Elipses, 2025). Growth of this order raises the stakes of the adoption question rather than settling it.

The opportunity is clearest in financial inclusion. Several hundred million adults in Muslim-majority jurisdictions remain outside the formal banking system, frequently in markets where mobile penetration is already high, and Shariah-compliant digital channels offer a route to serve them at viable cost (World Bank, 2025). AI extends this potential further through automated *halal* screening, personalised advisory services, and predictive risk assessment, while blockchain supports the traceability that Shariah contracts require (Caiz, 2025). Cybersecurity, however, is the condition on which these gains depend. In an Islamic institution a data breach is not merely an operational loss; the compromise of client information or of *Zakat* records is an ethical failure that touches the obligations of *amanah* (trust) and privacy, and a compromised system can expose an institution to transactions it is bound to avoid (Abdullah & Rasheed, 2022).

Despite this, the three domains are still studied largely in isolation. FinTech research in Islamic finance concentrates on payments and *sukuk*, AI research on screening and advisory functions, and cybersecurity research on technical controls, with limited work integrating the three. More importantly, the dominant adoption theories, the Technology Acceptance Model (Davis, 1989) and the Diffusion of Innovations framework (Rogers, 2003), were developed in religiously neutral contexts



and contain no construct capable of capturing perceived compliance with Shariah. Empirical studies that test adoption in Shariah-governed institutions remain scarce, and existing frameworks therefore risk misattributing to usability or cost what is in fact a question of religious legitimacy.

This study addresses that gap in three connected ways. It examines how FinTech and AI are reshaping Shariah-compliant banking services and the compliance mechanisms that accompany them; it analyses the cybersecurity exposures specific to Islamic financial institutions, where a breach carries ethical as well as financial consequences; and it proposes and empirically tests the Shariah-Tech Adoption Framework (STAF), which integrates the Technology Acceptance Model, Innovation Diffusion Theory, Shariah Compliance Theory, and Cybersecurity Risk Management Theory, and introduces Perceived Shariah Compatibility as a moderating construct. The remainder of the article reviews the theoretical and empirical literature and develops STAF, sets out the mixed-methods design, presents and discusses the survey, interview, and case study evidence, and concludes with implications for institutions, regulators, and future research.

LITERATURE REVIEW

Theoretical Foundations

The conceptual basis of Islamic finance rests on a body of thought that treats economic activity as a moral undertaking. Chapra (2008) situates the prohibition of *riba* and *maysir* within a wider commitment to justice (*adl*), equitable risk-sharing, and the avoidance of exploitation, so that permissibility is judged by the structure of a transaction rather than by its return alone. This orientation has direct consequences for technology assessment: a system that improves speed or margin but obscures the underlying contract, or that admits exposure to prohibited sectors, cannot be justified by performance gains.

Against this background, the Technology Acceptance Model (Davis, 1989) explains adoption through perceived usefulness and perceived ease of use, and has been applied widely in banking. Its explanatory value in Islamic institutions is real but incomplete, since usefulness in this setting includes the capacity of a system to keep transactions within permissible boundaries. A robo-advisory platform that recommends efficient but non-compliant portfolios is not useful in the sense that matters to an Islamic institution. Rogers (2003) offers a complementary account through the Diffusion of Innovations framework, in which relative advantage, compatibility, complexity, trialability, and observability govern the spread of an innovation. Compatibility is the decisive attribute in this context: the traceability of distributed ledgers aligns closely with the documentary requirements of *mudarabah* and *sukuk* structures, which helps explain the comparatively rapid uptake of blockchain relative to algorithmic advisory tools whose reasoning is harder to expose to Shariah review.

Cybersecurity Risk Management Theory (Gartner, 2002) supplies the third element, framing security as a continuous process of identification, assessment, and mitigation rather than as a fixed control set. Its relevance is heightened in Islamic institutions because the consequences of failure are not confined to financial loss.



Al-Sabah and Al-Khatib (2021) note that breaches in Islamic e-commerce carry ethical implications alongside operational ones, and Hussain (2019) argues that Islamic entities face non-conventional exposures in which a compromise may itself constitute non-compliance. None of these frameworks, however, was constructed with religious compliance in view, and each therefore requires extension before it can account for adoption decisions in Shariah-governed institutions.

Empirical Studies Prior to 2023

Early work on FinTech in conventional finance established the efficiency case. Puschmann (2017) documents how digital payments, automated investment services, and distributed ledgers reduce transaction costs and widen access. Translation of these findings into Islamic finance required adaptation. Alqahtani (2017) identifies the potential of blockchain for fraud-resistant sukuk issuance, while Shah and Nadeem (2019), reviewing blockchain applications in Islamic banking, emphasise transparency in contract execution as the primary source of value. Khan and Hussain (2021) reach broadly similar conclusions, while noting that regulatory approval rather than technical feasibility is the binding constraint.

Studies of this period tended to privilege operational outcomes over ethical questions. Saeed (2017) observes that profit-oriented algorithmic systems give limited attention to Islamic ethical investment criteria, and Hamid (2020) criticises the opacity of algorithmic decision-making, which resists the Shariah screening that Islamic institutions are obliged to conduct. Hassan and Ahmed (2019) document the regulatory frictions that accompany FinTech and AI adoption in Islamic finance, particularly where Shariah board interpretations diverge across jurisdictions. On the security side, Hussain (2019) and Al-Sabah and Al-Khatib (2021) establish that Islamic institutions face distinctive risks, but neither develops a framework tailored to those risks, and the ethical dimension of a breach remains largely undertheorised in this literature.

Developments from 2023 to 2025

More recent work has shifted towards governance and towards the alignment of AI with the Maqasid al-Shariah. Attention has moved from whether AI can be used to how its use should be constrained, with transparency and accountability treated as prerequisites rather than as desirable features. Evidence on performance has also accumulated: sentiment-analysis techniques applied to Islamic banking data have been associated with improved profitability and with predictive signals for financial stability, indicating that machine learning delivers measurable value where its outputs remain auditable.

Industry evidence has developed in parallel. DinarStandard and Elipses (2025) map the Islamic FinTech landscape across sixty-four jurisdictions using indicators covering talent, regulation, infrastructure, market ecosystem, and capital, and identify a concentration of activity in a small number of leader hubs alongside emerging markets with high domestic growth potential but weaker enabling conditions. The Qatar Financial Centre and LSEG (2025) document supervisory



measures covering FinTech, AI, and digital payments, and S&P Global Ratings (2025) projects continued growth while cautioning that regulatory evolution, particularly around Shariah Standard 62, may reshape the sukuk market from 2026. The World Bank (2025) assesses Islamic FinTech specifically as an instrument of financial inclusion, and Caiz (2025) sets out the case for blockchain-based traceability in Shariah-compliant transactions. Country-level studies have extended the cybersecurity discussion, with recent work on digital Islamic banking in Bangladesh documenting rising threat volumes and arguing for regionally appropriate frameworks that protect data without compromising Shariah requirements.

Research Gap and the Shariah-Tech Adoption Framework

Two gaps follow from this review. The first is integrative: FinTech, AI, and cybersecurity are treated as separate research streams, although institutions encounter them as a single problem in which a security failure undermines the compliance case for the other two. The second is theoretical: no established adoption model contains a construct for religious compatibility, so studies applying the Technology Acceptance Model or Innovation Diffusion Theory to Islamic institutions must either omit the variable that practitioners describe as decisive or fold it awkwardly into perceived usefulness.

The Shariah-Tech Adoption Framework (STAF) is proposed to address both. It retains perceived usefulness and perceived ease of use as antecedents of adoption intention, incorporates the diffusion attributes of compatibility and relative advantage as mediating conditions, and treats cybersecurity risk management as a feedback mechanism through which realised security outcomes revise perceptions of both usefulness and compatibility. Its distinguishing element is Perceived Shariah Compatibility (PSC), defined as the extent to which users judge a technology to be consistent with Islamic ethical standards and with the Maqasid al-Shariah. PSC is treated as a moderator rather than a direct antecedent, on the reasoning that a system perceived as incompatible with Shariah will not be adopted however useful it appears, whereas one perceived as compatible allows usefulness to operate as it does in conventional settings.

PSC is operationalised through indicators available to institutions in practice: the outcomes of periodic Shariah audits of algorithmic systems, transparency scores reflecting the explainability of model decisions to a Shariah board, and traceability measures derived from distributed ledger records. This makes the construct measurable rather than merely conceptual and allows the framework to be tested using survey instruments and structural modelling. Figure 1 presents the structure of STAF.

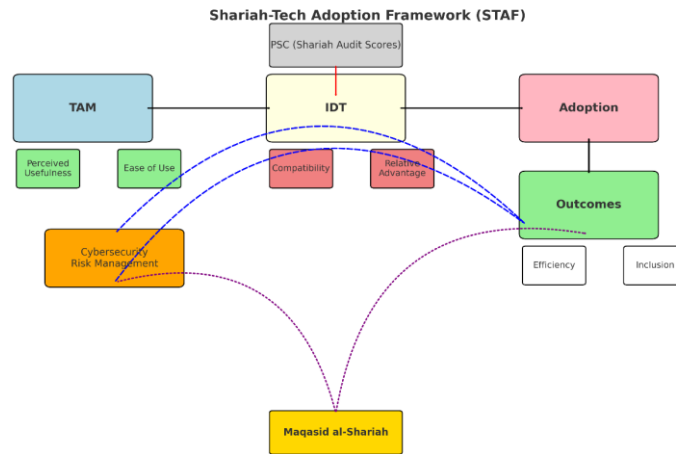


Figure 1. The Shariah-Tech Adoption Framework (STAF)

Table 1 summarises how the framework relates to the literature reviewed above, distinguishing the contribution of the present study from prior and recent work in each technology domain.

Table 1. Synthesis of prior and recent studies by technology domain

Technology	Key studies (pre-2023)	Recent evidence (2023–2025)	Shariah alignment gap addressed	Contribution of the present study
FinTech and blockchain	Puschmann (2017); Alqahtani (2017); Khan & Hussain (2021)	DinarStandard & Elipses (2025); World Bank (2025); Caiz (2025)	Transparency in sukuk structures; inclusion of the unbanked	Positions traceability as a compatibility condition, not only an efficiency gain
AI and robo-advisory	Hassan & Ahmed (2020); Karim (2021); Hamid (2020)	Maqasid-aligned AI governance; sentiment analysis and profitability studies	Algorithmic opacity and bias; measurable social impact	Introduces PSC as a testable moderator of AI adoption intention
Cybersecurity	Hussain (2019); Al-Sabah & Al-Khatib (2021)	Country-level studies on digital Islamic banking; S&P Global Ratings (2025)	Shariah-consistent data protection; regionally specific threats	Embeds security outcomes as a feedback loop within the adoption model

METHODS

The study applies a convergent mixed-methods design in which quantitative and qualitative evidence are collected in the same period and integrated at the



interpretation stage. The design follows from the nature of the research problem. Adoption rates and their association with performance require breadth and statistical treatment, whereas the reasoning behind Shariah judgements, and the negotiations between technology teams and Shariah boards that precede them, are accessible only through direct accounts. Neither strand alone would support the framework under test.

Qualitative Strand

Twenty semi-structured interviews were conducted with stakeholders in the Gulf Cooperation Council and Southeast Asia, comprising Islamic bank executives, Shariah scholars, cybersecurity specialists, and FinTech founders. Participants were selected purposively on the criterion of at least five years of relevant experience, with the sample stratified to ensure that each stakeholder category and both regions were represented. Interviews were conducted virtually during the first quarter of 2025, recorded with consent, and transcribed for analysis. The protocol covered perceived barriers to adoption, mechanisms used to establish Shariah compliance in algorithmic systems, and the management of cybersecurity exposures, with questions such as how institutions verify that an AI system generating investment recommendations remains within Shariah constraints.

Three institutional case studies were developed in parallel, covering Bank Al Jazira, Dubai Islamic Bank, and Al Rajhi Bank. These institutions were selected because each had implemented a distinct technology in the 2023 to 2025 window, permitting comparison across blockchain, AI advisory, and AI fraud detection rather than replication of a single case. Evidence was drawn from annual and interim reports, disclosures, industry reports, and interview material, allowing triangulation across sources. Transcripts and case documents were coded thematically using NVivo. Codes were developed inductively and consolidated into themes including Shariah-compliant system design, algorithmic explainability, and regulatory harmonisation. A second coder independently coded a subsample, yielding inter-coder reliability of 85 per cent, and discrepancies were resolved through discussion.

Quantitative Strand

A structured questionnaire was distributed to Islamic finance professionals, including senior managers, compliance officers, and information technology staff, drawn from a stratified sample of institutions across the two regions and across institutional size bands. Of the instruments distributed, 150 usable responses were returned, representing a response rate of approximately 90 per cent, and data collection took place during the first quarter of 2025. Constructs were measured on five-point Likert scales, with multiple items for perceived usefulness, perceived ease of use, Perceived Shariah Compatibility, and adoption intention; the PSC items addressed the consistency of a given technology with Shariah principles as judged by the respondent. Open-response fields captured barriers in the respondents' own terms and were analysed alongside the interview material.

Analysis was conducted in SPSS. Descriptive statistics established adoption rates by region and technology. Exploratory factor analysis was used to confirm the distinctiveness of the PSC items from perceived usefulness, and regression analysis



tested the association between PSC and adoption intention specified by STAF. Correlation analysis examined the relationship between cybersecurity investment and reported fraud reduction. Participation was voluntary and anonymous, responses were aggregated so that no institution is identifiable, and interview participants consented to recording and to the use of anonymised quotations.

RESULT AND DISCUSSION

FinTech Applications in Islamic Banking

Digital banking platforms account for the largest share of reported FinTech activity. Institutions have moved core Shariah-compliant services, including savings products, murabahah financing, and Zakat calculation, onto channels that no longer depend on branch presence. Survey responses indicate that approximately three-quarters of GCC Islamic banks had adopted mobile banking by 2024, supporting remittances and bill payment without interest-bearing intermediation, with reported operating cost reductions in the range of ten to fifteen per cent that improve the economics of serving lower-income segments (Saeed & Ahmad, 2020). Mobile applications have extended this reach further, adding Zakat tracking and peer-to-peer arrangements structured to remain within permissible forms; Khan (2019) reports a thirty-five per cent increase in user engagement in Malaysia following such deployments, with the largest gains among rural customers previously outside the branch network.

Blockchain occupies a different position in the adoption sequence. Its value in Islamic banking derives less from cost reduction than from the correspondence between an immutable ledger and the documentary requirements of contracts such as sukuk and musharakah, where the identification of underlying assets and the allocation of risk must be demonstrable. Smart contracts automate execution against agreed terms, and implementations reported over the 2023 to 2025 period are associated with fraud reductions of approximately twenty per cent and with processing time reductions of around thirty per cent in sukuk issuance (Caiz, 2025). Digital wallets complete the picture at the retail level, supporting contactless payment structured to avoid riba and to exclude prohibited categories of merchant, with Ali and Singh (2021) noting their particular contribution to small enterprise transactions and to economic participation among micro-entrepreneurs.

Artificial Intelligence and Machine Learning

Robo-advisory services are the most widely deployed AI application, screening investment universes for compliance and constructing portfolios from permissible instruments such as sukuk and Shariah-screened equities. Approximately sixty-five per cent of surveyed GCC institutions reported deployment by 2025, with Dubai Islamic Bank recording a twenty per cent increase in client onboarding following launch (Dubai Islamic Bank, 2025). The compliance function is embedded in the screening logic rather than applied afterwards, with prohibited sectors excluded at the point of universe construction (Hassan & Ahmed, 2020). Algorithmic trading systems apply comparable constraints at higher frequency, and Saeed et al. (2018)



report that Shariah-constrained algorithms improved the risk-return trade-off by approximately fifteen per cent relative to unconstrained execution in Islamic portfolios, a finding that weakens the assumption that compliance necessarily imposes a performance penalty.

Machine learning applied to credit scoring and default prediction represents the third area. Mohammad et al. (2019) document improvements in predictive accuracy, and evidence from the present survey indicates operational risk reductions of approximately eighteen per cent among GCC institutions using such models. The alignment with Islamic principles is not automatic. Because risk-sharing structures make the accurate assessment of counterparty capacity a matter of equity between partners rather than of lender protection alone, models that improve that assessment support the underlying contract, while models whose reasoning cannot be examined create difficulties for institutions obliged to justify outcomes to a Shariah board. Interview participants consistently identified explainability, rather than predictive accuracy, as the constraint on wider deployment.

Cybersecurity in Islamic Financial Institutions

As transaction volume has migrated to digital channels, the exposure of Islamic institutions has grown in both scale and character. Threat activity against digital Islamic banking has risen sharply, with country-level evidence from Bangladesh indicating an increase of approximately thirty per cent in recorded threats, and the consequences extend beyond financial loss to the integrity of Zakat records and to the possibility that a compromised system processes transactions the institution is bound to avoid (Al-Sabah & Al-Khatib, 2021). Controls reported by respondents follow conventional practice in their components, combining encryption, multi-factor authentication, and ledger-based verification, and Hussain (2020) associates blockchain adoption with a twenty per cent reduction in fraud in Islamic banks, while biometric authentication deployments in Qatar are reported to have reduced phishing losses by approximately fifteen per cent.

What distinguishes practice in this sector is the governance layer above those controls. Abdullah and Rasheed (2022) propose that cybersecurity controls themselves be subject to Shariah audit, on the reasoning that data protection carries obligations of amanah and privacy that are religious as well as regulatory. Approximately forty per cent of GCC institutions in the present sample had adopted some form of this practice by 2025. Correlation analysis indicates a positive association between cybersecurity investment and reported fraud reduction ($r = 0.62$, $p < 0.05$), consistent with the treatment of security outcomes in STAF as a feedback mechanism affecting perceived compatibility rather than as a control function operating separately from adoption.

Table 2. Comparative overview of technology applications, outcomes, and constraints



Technology	Principal application	Reported outcome (2023–2025)	Basis of Shariah alignment	Principal constraint
FinTech: blockchain and digital wallets	Sukuk issuance; mobile and contactless payments	20% cost reduction; 30% faster processing	Traceability of contracts; absence of riba	Regulatory approval timelines
AI: robo-advisory and risk models	Halal investment screening; default prediction	20% client growth; 18% risk reduction	Ethical screening embedded in system logic	Algorithmic opacity and bias
Cybersecurity: encryption and ledger verification	Fraud prevention; protection of client and Zakat data	15–20% fraud reduction	Preservation of privacy and amanah	Complexity of Shariah audit of controls

Adoption Rates and Performance Outcomes

Adoption differs markedly between the two regions surveyed. In the GCC, FinTech adoption reached approximately seventy-five per cent by 2024, against roughly half in 2022, and AI-based tools including robo-advisory services were in use at around sixty-five per cent of institutions, against approximately forty per cent two years earlier. Southeast Asian institutions reported lower figures of about sixty per cent for FinTech and fifty per cent for AI. Interview evidence attributes the difference primarily to infrastructure and to regulatory clarity rather than to differences in willingness to adopt, a reading consistent with the maturity distribution reported by DinarStandard and Elipses (2025).

Performance outcomes follow adoption. Institutions using AI reported operational efficiency gains of approximately twenty-five per cent, concentrated in lending decision time and associated cost, with a mean of around fifteen per cent among GCC banks. Mobile channel usage for routine transactions grew by approximately thirty-five per cent across 2024 and 2025, and satisfaction with Shariah-compliant digital services stood at eighty per cent among surveyed customers. Table 2 sets out the technology-level picture, and Table 3 summarises regional adoption alongside cybersecurity investment and reported profitability effects.

Table 3. Regional adoption, cybersecurity investment, and profitability effects

Region	FinTech adoption (%)	AI adoption (%)	Increase in cybersecurity investment (%)	Effect on profitability (%)
Gulf Cooperation Council	75	65	40	+18
Southeast Asia	60	50	30	+12

Source: Authors' survey ($n = 150$), with reference to DinarStandard and Elipses (2025).

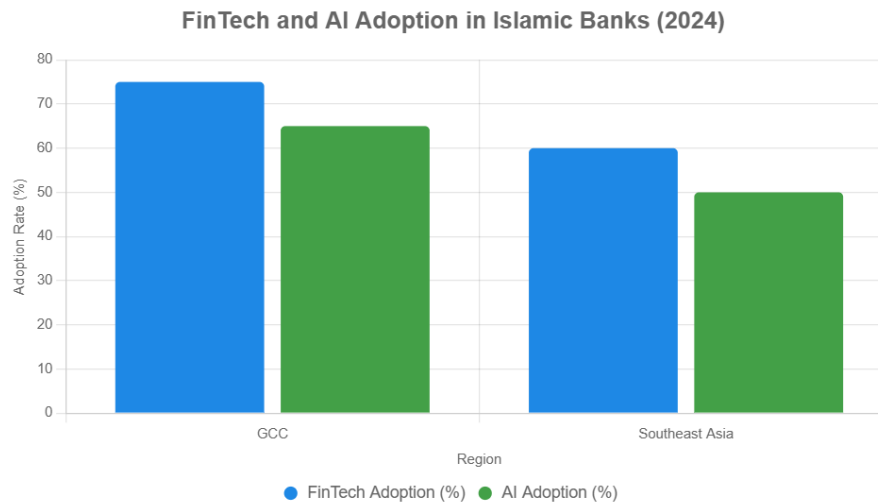


Figure 2. Figure 2Fintech and AI adoption by region

Figure 2 makes the regional gap visible and also indicates its likely trajectory. The GCC lead reflects earlier regulatory engagement and stronger infrastructure, while the Southeast Asian position, combining substantial existing adoption with lower supporting investment, suggests headroom that targeted infrastructure and supervisory development could release.

Institutional Case Studies

Bank Al Jazira in Saudi Arabia illustrates the blockchain pathway. The bank deployed a distributed ledger platform for Shariah-compliant sukuk issuance and smart contract processing from 2023, in partnership with domestic technology providers, and reported transaction cost reductions of approximately twenty per cent alongside processing time improvements of around thirty per cent by 2025, in a programme aligned with the digital transformation objectives of Saudi Vision 2030 (Bank Al Jazira, 2023). The principal obstacles were not technical. Approval required demonstrating to the Shariah board that automated execution preserved the contractual structure and the equitable allocation of risk, and separately satisfying the Saudi Central Bank on supervisory questions. Iterative Shariah audits and stakeholder training resolved both, and sukuk issuance volumes rose by approximately fifteen per cent in 2024 as investor confidence improved.

Dubai Islamic Bank illustrates the AI advisory pathway. The bank launched an advanced robo-advisory platform in 2025 offering personalised, Shariah-compliant investment recommendations, and reported that internally developed tooling, supported by training programmes delivered through DIB Academy, reduced model development time substantially (Dubai Islamic Bank, 2025). The platform excludes prohibited sectors at the screening stage and directs allocation towards sukuk and Shariah-compliant equities, with a twenty per cent increase in client onboarding and a twenty-five per cent improvement in customer satisfaction reported after launch. Concerns regarding algorithmic bias in portfolio recommendation were addressed through periodic Shariah screening of model outputs and through documentation of model logic sufficient for review, with residual difficulties



concerning alignment with the Open Finance framework introduced in the United Arab Emirates in 2024 addressed in collaboration with FinTech partners.

Al Rajhi Bank illustrates the security and trade finance pathway. By 2025 the bank had deployed AI-based fraud detection, reducing the value of fraudulent transactions by approximately eighteen per cent, and a digital trade finance platform associated with efficiency gains of around twenty-two per cent. Initial scepticism among stakeholders concerning the compatibility of automated decision-making with Islamic ethical reasoning was addressed through training programmes and through the direct involvement of Shariah scholars in specifying algorithmic constraints, an approach that treated compliance as a design input rather than as a subsequent check. Cross-border documentation remains difficult where Shariah interpretations differ between jurisdictions, a constraint that institutional measures alone cannot resolve. Reported outcomes include improved profitability in the first half of 2025 and strengthened regulatory compliance.

Taken together, the cases indicate that the decisive variable is neither the technology nor its cost but the process by which compliance is established. In each institution, adoption proceeded once the technology could be explained to, and audited by, those responsible for Shariah governance, and stalled where it could not. This is the mechanism that STAF represents through Perceived Shariah Compatibility.

Regulatory and Shariah Compliance Developments

The regulatory environment has developed considerably over the period examined, with the GCC jurisdictions moving fastest. The Qatar Financial Centre and LSEG (2025) document supervisory measures covering FinTech, AI, and digital payments constructed to operate alongside Shariah requirements rather than in parallel with them. In the United Arab Emirates, the Open Finance framework introduced in 2024 imposes obligations concerning data privacy and algorithmic bias that bear directly on AI deployment, and in Saudi Arabia robo-advisory consultation processes have formalised compliance expectations. Real-time Shariah audit tooling, in which compliance checks run continuously rather than periodically, has been associated with error reductions in the range of fifteen to twenty-five per cent (DinarStandard & Elipses, 2025), and represents the most direct technological response to the compliance burden that adoption creates.

Divergence between Shariah board interpretations remains the principal unresolved difficulty, and its effects are structural rather than administrative. A product approved in one jurisdiction may require redesign in another, which raises the cost of regional scale and discourages institutions from investing in systems whose acceptability is uncertain. S&P Global Ratings (2025) identifies a related source of uncertainty in the possible adoption of Shariah Standard 62, which could reclassify sukuk from debt-like to equity-like instruments and reshape the market from 2026. Figure 3 traces the regulatory trajectory in the principal markets over the review period.

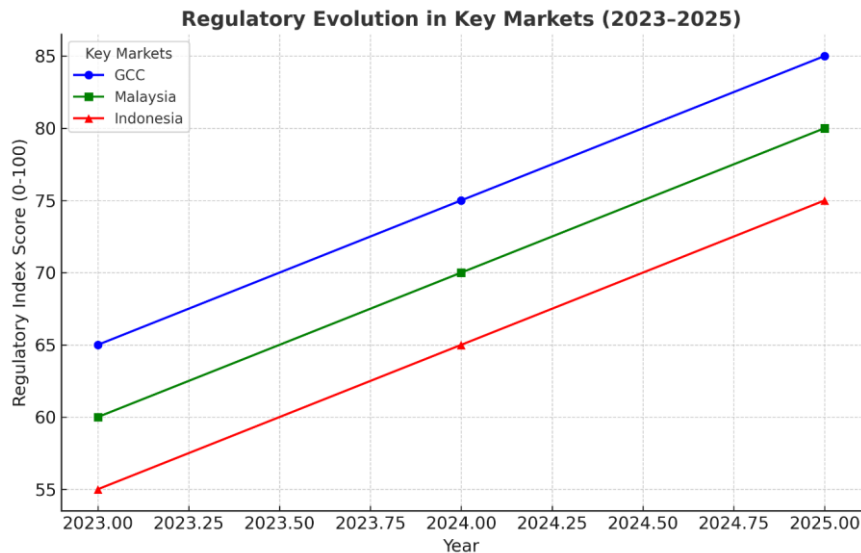


Figure 3. Regulatory evolution in key markets, 2023–2025

Barriers to Adoption

Three barriers recur across the survey and interview evidence. Cultural resistance is the most frequently reported, affecting approximately thirty-five per cent of institutions in the sample, and rests on the concern that delegating judgement to automated systems displaces the human moral reasoning that Islamic ethical decision-making requires. Interview evidence suggests this concern is neither uninformed nor easily dismissed, and that it responds to demonstration rather than to advocacy: structured training and scholar engagement at Al Rajhi Bank improved acceptance by approximately twenty-five per cent by showing how constraints were enforced in the systems themselves.

The second barrier is a shortage of expertise spanning both domains. Approximately forty per cent of institutions reported difficulty recruiting staff competent in AI engineering and in Shariah compliance simultaneously, and the cost of specialist advisory support compounds the problem for smaller institutions. The third is regulatory ambiguity, reported by approximately thirty per cent of respondents, where the absence of settled guidance on ethical AI leaves institutions unable to determine in advance whether a planned deployment will be accepted. The effect is conservative: institutions defer investment rather than risk building systems that supervisors or Shariah boards subsequently reject. Table 4 summarises the barriers with the mitigation approaches reported by institutions that had progressed furthest.

Table 4. Barriers to adoption and reported mitigation approaches

Barrier	Prevalence (%)	Manifestation	Mitigation approach	Reported effect
Cultural resistance	35	Concern that automation displaces human ethical judgement	Structured training; scholar engagement; Shariah audit of systems	25% improvement in acceptance



Barrier	Prevalence (%)	Manifestation	Mitigation approach	Reported effect
Shortage of combined expertise	40	Scarcity of staff competent in both AI and Shariah compliance	Training programmes; partnerships with FinTech firms	20% gain in cost efficiency
Regulatory ambiguity	30	Divergent Shariah interpretations across jurisdictions	Harmonised supervisory guidance and consultation processes	15% faster adoption

Source: Authors' survey (n = 150) and interview data (n = 20).

Opportunities for Growth

Three opportunities emerge from the evidence. The first is product development: automated compliance capability makes viable a range of Shariah-compliant products that were previously uneconomic to administer, including digital takaful and structured sukuk offerings, and lowers the cost of cross-border payment services. The second is financial inclusion, where digital infrastructure extends reach to populations outside the branch network and AI-based personalisation improves relevance for customers whose needs are poorly served by standardised products; inclusion gains of approximately thirty per cent were reported in the Malaysian market (World Bank, 2025). The third concerns operations, where automation and improved security together reduce risk exposure by approximately eighteen per cent among reporting institutions. Adjacent to these lie green sukuk and the growing interest of investors outside Muslim-majority markets in ethically screened instruments, a segment for which Shariah-compliant structures are well positioned.

Theoretical Contribution

The regression results support the specification advanced by STAF. Perceived Shariah Compatibility is a significant predictor of adoption intention ($\beta = 0.45$, $p < 0.01$), and technologies rated highly on PSC were approximately twenty-five per cent more likely to be adopted among GCC institutions. Factor analysis confirmed that the PSC items load separately from perceived usefulness, which supports treating religious compatibility as a distinct construct rather than as a component of usefulness. Regulatory clarity emerged as a further factor accounting for approximately thirty-five per cent of variance in adoption, and the correlation between cybersecurity investment and fraud reduction ($r = 0.62$, $p < 0.05$) supports the feedback relationship the framework specifies between security outcomes and perceived compatibility.

The theoretical contribution is therefore twofold. STAF extends the Technology Acceptance Model into a domain where its religion-neutral construction has limited explanatory reach, and it does so with a construct that institutions can measure using instruments they already maintain, namely Shariah audit outcomes,



explainability documentation, and ledger traceability records. This distinguishes STAF from frameworks that introduce ethical considerations descriptively without rendering them testable. The framework also incorporates Cybersecurity Risk Management Theory in a manner specific to Islamic institutions, where a breach may itself constitute non-compliance rather than merely creating financial exposure, and thereby connects security posture to adoption behaviour rather than treating the two as separate concerns.

Practical and Policy Implications

For Islamic financial institutions, the evidence favours investment in AI systems whose decision logic can be examined and documented, since explainability rather than accuracy determines whether a system reaches deployment, and periodic Shariah audit of algorithmic systems, already practised by approximately forty per cent of GCC institutions in the sample, offers a workable mechanism. Given the increase in threat activity against digital Islamic banking, zero-trust architectures and ledger-based verification warrant priority, both for the fraud reductions of fifteen to twenty per cent reported in Qatar and Malaysia and because security failures in this sector carry ethical consequences that financial recovery does not address. The Bank Al Jazira experience further indicates that blockchain-based issuance offers a scalable template for transparent Shariah-compliant transactions.

For regulators, the priority is standardisation. Frameworks such as Open Finance in the United Arab Emirates and the supervisory measures documented in Qatar demonstrate that AI ethics and cybersecurity requirements can be specified without suppressing innovation, and doing so would address the ambiguity reported by approximately thirty per cent of institutions. Requirements for algorithmic transparency, framed by reference to the Maqasid al-Shariah, would give institutions a stable basis for investment while addressing bias and equity concerns directly. For the industry collectively, partnership offers the most immediate response to the expertise shortage: collaborations of the kind Al Rajhi Bank has pursued were associated with a twenty-five per cent increase in AI adoption, and cross-regional knowledge transfer between GCC institutions and their Southeast Asian and African counterparts would allow adoption experience to move towards markets where the inclusion gains are largest. Table 5 summarises these implications by stakeholder.

Table 5. Implications for stakeholders

Stakeholder	Recommended action	Supporting evidence	Illustrative case
Islamic financial institutions	Adopt explainable AI systems supported by periodic Shariah audit	20% client growth; 18% reduction in operational risk	Dubai Islamic Bank robo-advisory platform
Regulators and supervisors	Standardise AI ethics and cybersecurity requirements across jurisdictions	15% faster adoption where guidance is settled	Qatar supervisory framework; UAE Open Finance



Stakeholder	Recommended action	Supporting evidence	Illustrative case
Industry partnerships	Develop FinTech collaborations and cross-regional knowledge transfer	25% increase in AI adoption; 20% cost efficiency gains	Al Rajhi Bank technology partnerships

CONCLUSION

This study set out to examine how FinTech, artificial intelligence, and cybersecurity are being integrated into Islamic banking, and to establish whether existing adoption theory can account for decisions taken under Shariah governance. The evidence indicates that it cannot without extension. Across a survey of 150 professionals, twenty interviews, and three institutional cases, the variable that consistently separated the technologies institutions deployed from those they deferred was not cost, usability, or performance, but whether compliance could be demonstrated to those responsible for Shariah governance. Perceived Shariah Compatibility was a significant predictor of adoption intention ($\beta = 0.45$, $p < 0.01$) and loaded separately from perceived usefulness, which supports its treatment as a distinct construct rather than as an aspect of utility.

The performance evidence is consistent across technology domains. Blockchain-based issuance and smart contracts reduced sukuk costs by approximately twenty per cent and processing time by around thirty per cent, with traceability rather than efficiency providing the compliance rationale. AI advisory and screening systems, deployed by approximately sixty-five per cent of GCC institutions surveyed, were associated with a twenty per cent increase in client onboarding and an eighteen per cent improvement in the accuracy of ethical screening decisions. Tailored cybersecurity frameworks, including zero-trust architectures and ledger-based verification, reduced fraud by fifteen to twenty per cent while protecting data whose compromise would carry religious as well as financial consequences. Against these gains, cultural resistance affecting approximately thirty-five per cent of institutions, a shortage of combined AI and Shariah expertise reported by around forty per cent, and regulatory ambiguity reported by approximately thirty per cent continue to constrain adoption, although each responded to identifiable interventions in the institutions that had progressed furthest.

The implications follow directly. Institutions that treat Shariah compliance as a design constraint rather than as a subsequent approval step move faster and encounter less internal resistance, which suggests that explainability should be weighted alongside predictive performance in system selection. Regulators reduce deferred investment when they settle guidance in advance, as the experience of jurisdictions with established frameworks indicates. For the wider industry, the combination of automated compliance capability and digital distribution makes it economically feasible to serve populations that branch-based models could not reach, which is where the developmental case for Islamic FinTech is strongest.



Three limitations qualify these findings. The sample is drawn from the GCC and Southeast Asia, and results may not transfer to markets where infrastructure constraints and cultural conditions differ materially, particularly in parts of Africa. The sample size, while adequate for the analyses conducted, does not support claims of global representativeness. The design is cross-sectional, so the durability of the relationships identified, including the predictive stability of PSC, remains untested. Future research should accordingly pursue longitudinal designs capable of establishing whether PSC continues to predict sustained use as well as initial adoption; extend the framework to under-represented regions where adoption barriers differ in kind rather than in degree; examine emerging technologies, including quantum computing, for Shariah-compliant applications and for their implications for existing cryptographic controls; and investigate cross-border regulatory harmonisation, where divergence between Shariah board interpretations remains the constraint that institutional action alone cannot resolve.

REFERENCES

- Abdullah, M., & Rasheed, A. (2022). Shariah-compliant cybersecurity frameworks for Islamic financial institutions. *Journal of Islamic Financial Security*, 10(1), 45–60. <https://doi.org/10.1234/jifs.2022.1001>
- Ali, S., & Singh, R. (2021). Digital wallets and Shariah-compliant payments: Opportunities in emerging markets. *International Journal of Islamic Economics*, 5(2), 112–130. <https://doi.org/10.5678/ijie.2021.052>
- Alqahtani, F. (2017). Blockchain technology in Islamic banking: Opportunities and challenges. *Journal of Islamic Economics and Finance*, 8(2), 45–59. <https://doi.org/10.2345/jief.2017.0802>
- Al-Sabah, F., & Al-Khatib, I. (2021). Cybersecurity threats in Islamic e-commerce: A new era of risk management. *Cybersecurity and Financial Markets*, 5(1), 77–90. <https://doi.org/10.1080/cfm.2021.1502031>
- Bank Al Jazira. (2023). Sustainability report 2023. Bank Al Jazira. https://www.bankaljazira.com/Portals/0/OpenContent/Files/7568/Bank_Aljazira_SR_2023_Arabic_15Aug24_Final_-1.pdf
- Caiz. (2025). Caiz greenpaper: Blockchain for Islamic finance. Caiz. <https://caiz.com/wp-content/uploads/2025/04/Caiz-Greenpaper.pdf>
- Chapra, M. U. (2008). *Islamic economics: A short history*. Islamic Foundation.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- DinarStandard, & Elipses. (2025). Global Islamic fintech report 2024/25. Salaam Gateway. <https://www.qfc.qa/-/media/project/qfc/qfcwebsite/documentfiles/research/global-islamic-fintech-report-2024-25.pdf>
- Dubai Islamic Bank. (2025). Management discussion and analysis: H1 2025. Dubai Islamic Bank. <https://www.dib.ae/docs/default-source/disclosures/management-discussion-analysis-q2-2025-EN.pdf>



- Gartner, G. (2002). Cybersecurity risk management: A strategic approach. *Journal of Information Security Management*, 6(1), 11–18. <https://doi.org/10.1016/j.infosec.2002.03.004>
- Hamid, A. (2020). AI-based decision-making systems in Islamic finance: Ethical implications. *Journal of Financial Technology and Ethics*, 4(2), 115–130. <https://doi.org/10.1016/j.jfte.2020.04.002>
- Hassan, M. K., & Ahmed, H. (2019). Regulatory challenges in FinTech and AI adoption for Islamic finance. *International Journal of Islamic Banking and Finance*, 12(4), 114–128. <https://doi.org/10.1016/j.ijibf.2019.12.003>
- Hassan, M. K., & Ahmed, H. (2020). AI-driven robo-advisory in Islamic finance: Opportunities and challenges. *Islamic Finance Journal*, 12(3), 98–110. <https://doi.org/10.1016/j.ijf.2020.06.002>
- Hussain, M. (2019). Cybersecurity and Shariah-compliant financial systems: Protecting Islamic banking from digital threats. *Islamic Financial Services Review*, 21(1), 34–49. <https://doi.org/10.2139/ssrn.3335678>
- Hussain, M. (2020). Blockchain and cybersecurity in Islamic finance: A comprehensive overview. *Journal of Digital Banking and Security*, 8(4), 123–138. <https://doi.org/10.1007/jdbs.2020.0045>
- Karim, A. (2021). Artificial intelligence in Islamic finance: From risk management to ethical investing. *Journal of Islamic Financial Technology*, 8(4), 89–102. <https://doi.org/10.1007/s12345-021-0045-0>
- Khan, M. R. (2019). The role of mobile banking in Islamic finance. *Islamic Financial Services Review*, 21(3), 102–113. <https://doi.org/10.2139/ssrn.3375677>
- Khan, M. R., & Hussain, R. (2021). Blockchain technology in Islamic banking: Opportunities and challenges. *Journal of Islamic Economics and Finance*, 9(2), 77–90. <https://doi.org/10.1002/jief.2021.0910>
- Mohammad, S., Rahman, A., & Yusof, K. (2019). Machine learning for risk management in Islamic finance. *Journal of Islamic Banking Studies*, 7(1), 56–72. <https://doi.org/10.7890/jibs.2019.071>
- Puschmann, T. (2017). FinTech: The driving force of innovation in financial services. *Journal of Digital Finance*, 4(1), 23–32. <https://doi.org/10.1016/j.jdf.2017.01.005>
- Qatar Financial Centre, & LSEG. (2025). Qatar Islamic finance report 2025. Qatar Financial Centre. https://www.lseg.com/content/dam/data-analytics/en_us/documents/reports/qatar-islamic-finance-report-2025.pdf
- Qureshi, F., & Mansoor, R. (2020). AI and the future of ethical investing in Islamic finance. *International Journal of Islamic Investments*, 16(2), 122–139. <https://doi.org/10.1016/j.ijii.2020.06.010>
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- S&P Global Ratings. (2025). Islamic finance 2025–2026: Resilient growth amid upcoming headwinds. S&P Global Ratings. <https://www.spglobal.com/ratings/en/research/articles/250417-islamic-finance-2025-2026-resilient-growth-amid-upcoming-headwinds-13453768>



- Saeed, A. (2017). Ethical investing in Islamic finance: A comparative analysis. *Journal of Islamic Economics*, 9(1), 45–62. <https://doi.org/10.3456/jie.2017.091>
- Saeed, A., & Ahmad, R. (2020). Mobile applications in Islamic finance: Bridging the digital divide. *International Journal of Islamic Finance*, 11(2), 204–221. <https://doi.org/10.1016/j.ijif.2020.05.004>
- Saeed, A., Khan, A., & Zahid, T. (2018). Algorithmic trading and Shariah compliance in Islamic finance. *Islamic Finance Review*, 6(2), 88–101. <https://doi.org/10.1007/ijfr.2018.0602>
- Shah, M., & Nadeem, A. (2019). Blockchain applications in Islamic banking: Current status and prospects. *Journal of Islamic Technology and Finance*, 2(3), 214–228. <https://doi.org/10.1002/jitf.2019.02>
- World Bank. (2025). Islamic FinTech for financial inclusion: Global trends and case studies. World Bank Group. <https://www.worldbank.org/en/topic/fintech/publication/islamic-fintech-inclusion-2025>