

Consumer Trust, Data Privacy, and Emerging Cybersecurity in Islamic Digital Banking: A Bibliometric and Systematic Review

Faria Zahan Sarna

faria.sarna@metrouni.edu.bd

Metropolitan University

NHM Hassan Imam Chowdhury

Standard Islami Bank PLC

Abdullah Al Himel

Military Institute of Science and Technology

Systematic Review

Keywords: Islamic Digital Banking, Consumer Trust, Data Privacy, Cybersecurity, Bibliometric Analysis, Protection Motivation Theory, Privacy Calculus, Islamic FinTech

Posted Date: October 12th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10093745/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Background.

Islamic banking is a systemic component of global capital markets, serving Muslim communities within a global Islamic finance industry whose assets are estimated in the trillions of United States dollars. Its rapid digital transformation creates a tension that scholarship has not resolved: Islamic jurisprudence obligates institutions to uphold *Amanah*, a binding duty of trustworthy stewardship that extends to protecting customers' financial data, yet the cybersecurity threats and data-privacy failures that imperil this duty are rarely examined in research on Islamic digital banking.

Methods.

This review presents an integrated bibliometric and systematic analysis of consumer trust, data privacy, and cybersecurity in Islamic digital banking. A structured Scopus search produced a final peer-reviewed corpus of 34 journal articles and review papers published between 2013 and 30 June 2025, drawn from 200 records through documented screening and eligibility assessment.

Results.

The corpus shows sustained growth in annual output, with the majority of papers appearing between 2021 and 2025. Three frameworks are absent from all 34 papers in the identified corpus: Protection Motivation Theory, Privacy Calculus, and any integrated model linking the higher objectives of Islamic law to security or privacy; cybersecurity and data privacy are rarely the primary research topic. A title-term co-word analysis reveals thematic clusters dominated by technology-adoption and relationship-trust research, with security- and privacy-oriented terms remaining peripheral.

Conclusions.

The review develops a three-layer conceptual framework and a six-proposition research agenda, offering a theoretically grounded basis for advancing cybersecurity and privacy scholarship in Islamic digital banking.

1 INTRODUCTION

Islamic banking has evolved from a niche ethical finance model into a systemic component of global capital markets. The global Islamic finance industry held approximately US\$4.5 trillion in assets in 2022 and is projected to approach US\$6.7 trillion by 2027, with Islamic banking accounting for about 72 per cent of that total (ICD-LSEG, 2023); the sector serves Muslim communities that numbered roughly two billion people, about a quarter of the world's population, in 2020 (Pew Research Center, 2025), and

commands institutional and regulatory attention at the highest levels (Islamic Financial Services Board [IFSB], 2024). The digital transformation that accelerated after 2018 has restructured how these consumers engage with their financial institutions. Mobile banking applications, internet-based transaction portals, and cloud-native Islamic FinTech platforms have progressively displaced the branch as the primary service interface. This technological shift introduces an underlying tension that the existing literature has not yet addressed. Within Islamic jurisprudence, digital financial operations are governed not merely by legal compliance but by the doctrine of *Amanah*, a binding obligation of trustworthy stewardship that requires an institution to protect every asset entrusted to it, including the financial data, transaction histories, and digital identities of its customers. The higher objectives of Islamic law, *Maqasid al-Shariah*, anchor this duty in *Hifz al-Mal*, the preservation of property, which contemporary scholars have extended to encompass digital information assets (Shinkafi, 2017). A data breach in this context is not merely a technical failure; the framework proposed in this review conceptualises it as a potential violation of the institution's *Amanah* obligation, rather than presenting this as an established jurisprudential fact. Yet cybersecurity threats, data privacy failures, and the psychological mechanisms through which Muslim consumers appraise and respond to these risks have rarely been examined within the scholarly discourse on Islamic digital banking. The empirical boundaries of this gap are established through a structured database analysis. A structured Scopus search of the broader Islamic FinTech ecosystem retrieves 200 records. Applying rigorous inclusion and exclusion criteria in accordance with Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines (Page et al., 2021) reduces this pool to a final corpus of 34 peer-reviewed journal articles and review papers published between 2013 and 30 June 2025. This progression from 200 records to a final corpus of 34 is consistent with an emerging and still-nascent research intersection.

Several recent reviews have examined adjacent territory. Shahimi et al. (2025) offer a comprehensive bibliometric mapping of FinTech research spanning 1968 to 2025, demonstrating the dominance of TAM and UTAUT frameworks without engaging cybersecurity or Islamic ethics as analytical constructs. Alsmadi (2025) investigates adoption determinants in Islamic FinTech without applying a bibliometric synthesis or examining data privacy or threat-response behaviour. Abakpa and Dvouletý (2025) explicitly identify the security layer as an under-researched dimension of enterprise architecture, providing direct empirical motivation for the present review. Unal (2022) offers a retrospective mapping of FinTech and blockchain in Islamic finance without engaging consumer trust or privacy dimensions. A recent systematic review of consumer behaviour in Islamic banking, covering 135 Scopus documents, maps adoption, satisfaction and loyalty themes but does not address cybersecurity or privacy (R.V. et al., 2024); the present review is positioned to complement, rather than duplicate, that work. Table 1 situates this review against the nearest prior contributions.

Table 1
Comparison of this review with the five nearest prior syntheses

Study (DOI)	Corpus	Method	Primary focus	Structural omission this review addresses
Shahimi et al. (2025) FBJ · DOI: 10.1186/s43093-025-00652-1	n = 2,760 (WoS)	Bibliometric (VOSviewer + PoP)	FinTech mapping 1968–2025; TAM/UTAUT dominant; blockchain emerging	No cybersecurity or privacy dimension; trust as static adoption antecedent; Islamic ethics absent
Alsmadi (2025) FBJ · DOI: 10.1186/s43093-025-00430-z	n = 263 (survey)	Quantitative (SmartPLS)	Islamic FinTech adoption Jordan; Shariah compliance and Islamic social responsibility	No bibliometric synthesis; cybersecurity and privacy absent; adoption under stable conditions only
Abakpa & Dvoutely (2025) FBJ · DOI: 10.1186/s43093-025-00659-8	n = 30 (articles)	Systematic literature review	Digitalization and financial performance; security layer flagged as under-researched	No Islamic finance focus; no consumer trust or privacy analysis; security identified as gap only
Koşti & Kayadibi (2025) FBJ · DOI: 10.1186/s43093-025-00602-x	n = 522 (Scopus)	Bibliometric (R+VOSviewer)	AI and ML in HRM; shift from technical to ethical HR dimensions	Domain is HRM not Islamic banking; no cybersecurity consumer behaviour
Unal (2022) Fintech · DOI: 10.3390/fintech1040029	Conceptual	Retrospective investigation	FinTech, digitalisation, blockchain in Islamic finance	No systematic synthesis; consumer trust and privacy absent; cybersecurity as technical feature only

Note. FBJ = Future Business Journal; PoP = Publish or Perish; TCCM = Theory, Context, Characteristics, Methodology; SPAR-4-SLR (Paul et al., 2021). The comparison is limited to the reviews most closely aligned with the present review's scope and is not an exhaustive census of Islamic finance reviews.

Study (DOI)	Corpus	Method	Primary focus	Structural omission this review addresses
This review Future Business Journal	n = 34 peer-reviewed 2013–30 June 2025	Bibliometric+TCCM SLR (SPAR-4- SLR+PRISMA 2020)	Consumer trust, data privacy, cybersecurity in Islamic digital banking; Maqasid integration with PMT and Privacy Calculus	Among the first at this intersection; confirms 0/34 PMT and Privacy Calculus absence; proposes three-layer framework with six testable propositions
<i>Note. FBJ = Future Business Journal; PoP = Publish or Perish; TCCM = Theory, Context, Characteristics, Methodology; SPAR-4-SLR (Paul et al., 2021). The comparison is limited to the reviews most closely aligned with the present review's scope and is not an exhaustive census of Islamic finance reviews.</i>				

The present study is organised around four research questions (RQs):

RQ1

How has scholarly production on consumer trust, data privacy, and emerging cybersecurity in Islamic digital banking evolved across geographic, institutional, and temporal boundaries, and what events coincide with key inflection points? Bibliometric performance analysis captures structural publication patterns that descriptive narrative reviews cannot quantify (Van Eck & Waltman, 2010).

RQ2

What are the dominant intellectual pillars, thematic clusters, and research fronts shaping the current discourse? Science mapping via title-term co-occurrence analysis renders the latent thematic architecture of a field visible (Van Eck & Waltman, 2014).

RQ3

How do Islamic ethical frameworks, specifically *Amanah*, *Hifz al-Mal*, and *Maqasid al-Shariah*, currently integrate, or fail to integrate, with Western behavioural trust and privacy models? TCCM-coded systematic review evaluates theory deployment and contextual patterns with sufficient granularity to answer a qualitative theoretical question (Paul & Criado, 2020).

RQ4

What multi-disciplinary framework and testable propositions can guide future inquiry into Shariah-compliant cybersecurity and consumer privacy behaviour? A research agenda matrix operationalises

identified gaps into propositions and matched methodologies (Paul et al., 2021).

This review makes three principal contributions. First, it maps the intellectual structure of consumer trust, data privacy, and cybersecurity research in Islamic digital banking through an integrated bibliometric and Theory, Context, Characteristics, and Methodology approach. Second, it documents three systematic theoretical omissions across the corpus, namely Protection Motivation Theory, Privacy Calculus, and any integrated *Maqasid al-Shariah* security model. Third, it synthesises these observations into a three-layer conceptual framework and a research agenda of six testable propositions. The remainder of this paper proceeds as follows. Section 2 develops the three-layer theoretical framework. Section 3 documents the methodology. Section 4 presents the performance analysis (RQ1). Section 5 reports the science mapping (RQ2). Section 6 applies the TCCM synthesis (Paul & Criado, 2020) to address RQ3. Section 7 presents the Research Agenda Matrix (RQ4). Section 8 states conclusions and limitations. Two constructs introduced in the framework that follows, the Shariah non-compliance risk amplifier and Perceived *Amanah* Alignment, are proposed conceptual lenses derived from the gaps identified in the review rather than empirical findings of the reviewed corpus; this distinction is signalled explicitly wherever the constructs appear.

2 THEORETICAL FRAMEWORK

The framework developed in this section emerges from the gaps the review subsequently documents in Section 6: the absence of threat-appraisal and privacy-decision models, and the lack of any operational link between *Maqasid al-Shariah* and digital security. Each layer below is presented as a response to one of these synthesised gaps rather than as an a priori model.

2.1 Defining the unit of analysis: Islamic digital banking

This review distinguishes between two distinct entities. The first is the legacy Islamic commercial bank, an established institution migrating traditional operations, asset-backed portfolios, and Shariah governance structures onto digital platforms. The second is the native Islamic FinTech platform, a cloud-born entity, including Shariah-compliant neo-banks, peer-to-peer financing platforms, and halal robo-advisors, that operates without physical branches. The systematic review in Section 6 indicates that twenty of the 34 papers study legacy Islamic banking contexts and five focus on native Islamic FinTech platforms, leaving the trust and privacy dynamics of native platforms comparatively under-examined (Dawood et al., 2022; Idrees et al., 2024). Throughout this review, the term Islamic digital banking is used as the umbrella category for both forms, while Islamic FinTech denotes the native platforms specifically.

2.2 Layer 1: *Maqasid al-Shariah* and the principle of *Amanah*

The normative anchor of the proposed framework, summarised in Fig. 1, is drawn from *Maqasid al-Shariah*, the higher objectives of Islamic law. Shinkafi (2017), among the most cited explicitly theoretical works in the present corpus (approximately 51 Google Scholar citations as at 30 June 2025), argues that

the preservation and equitable circulation of wealth constitute foundational obligations of any Shariah-compliant financial institution. Building on Hifz al-Mal as the preservation of property, this review proposes extending the principle conceptually to encompass a customer's digital footprint, transaction records, and financial identity as protected informational assets. *Hifz al-Aql* is deliberately excluded, its traditional application to the protection of intellect from moral and ideological corruption renders it theologically contestable as an information security construct.

Central to Layer 1 is the principle of *Amanah*, trustworthiness as a binding ethical obligation. The qualitative study of Ashraf et al. (2015) reports that consumer confidence in an Islamic bank's compliance with its ethical mandates functions as a trust benefit that is related to, but conceptually distinct from, standard Technology Acceptance Model (TAM) constructs; this offers related evidence that informs, without by itself validating, the present operationalisation.

Importantly, *Amanah* operates as a double-edged mechanism. Under normal conditions, visible adherence to Shariah governance may generate a proposed spiritual trust benefit, a degree of consumer loyalty that extends beyond utility calculations (Ashraf et al., 2015; Parayil Iqbal, 2023). When an institution suffers a data breach attributable to systemic negligence, this premium inverts. While service failure literature has long recognised that deep relational attachment amplifies perceived betrayal, the expectation-violation effect (Grégoire et al., 2009), to the best of our knowledge, this review is among the first to operationalise this inversion within an Islamic jurisprudential context, framing the breach as the transformation of a Shariah compliance asset into a Shariah non-compliance liability.

2.3 Layer 2: Protection Motivation Theory and the Shariah amplifier

Layer 1 feeds directly into Layer 2, which adapts Protection Motivation Theory (PMT) to model how Islamic digital banking consumers cognitively evaluate cybersecurity threats. Developed by Rogers (1975) and extended in Rogers (1983), PMT posits that protective behavioural intentions are determined by threat appraisal (perceived severity × vulnerability) and coping appraisal (response efficacy × self-efficacy). PMT is among the frameworks most frequently applied in information-security and technology-threat research, with numerous applications synthesised in the meta-analysis of Sommestad et al. (2015) (Rogers, 1975, 1983). Its absence from all 34 papers is theoretically noteworthy, suggesting that the field's reliance on adoption models has foreclosed engagement with frameworks specifically designed for threat environments.

The novel bridge introduced here is the Shariah non-compliance risk amplifier, a moderating construct through which Layer 1 shapes Layer 2 processing. When an Islamic digital banking consumer confronts a cybersecurity threat, the spiritual obligations embedded in *Amanah* may introduce an additional perceived severity dimension linked to Shariah compliance concerns. This amplification is proposed as a conceptual lens for future empirical testing and is not presented as a finding of this review.

2.4 Layer 3: Privacy Calculus and Perceived *Amanah* Alignment

Layer 1 feeds simultaneously into Layer 3, which situates consumer privacy decisions within the Privacy Calculus framework (Dinev & Hart, 2006). Privacy Calculus models the consumer's assessment of whether the benefits of disclosing personal information outweigh its associated privacy costs and is among the dominant models of privacy decision-making in information systems research (Dinev & Hart, 2006). Its omission across all 34 papers is, like the PMT gap, theoretically significant.

The bridge connecting Layer 1 to Layer 3 is Perceived *Amanah* Alignment, the consumer's subjective psychological confidence that the institution is actively fulfilling its *Amanah* obligation. A critical terminological distinction must be maintained: *Amanah* as treated in Layer 1 is the institution's structural and jurisprudential duty; Perceived *Amanah* Alignment is the consumer's psychological perception of that duty being met, a subjective and measurable construct. When Perceived *Amanah* Alignment is high, it may function as a non-monetary spiritual benefit that offsets privacy costs in the consumer's calculus (Ashraf et al., 2015). PMT explains how consumers appraise cybersecurity threats and form protective intentions; Privacy Calculus explains how they weigh privacy costs and benefits in deciding whether to engage. Together, these two frameworks capture complementary stages of consumer trust under cybersecurity uncertainty, the threat-response stage and the cost-benefit calculation stage, in a way that neither TAM nor the Unified Theory of Acceptance and Use of Technology (UTAUT) is designed to address (Davis, 1989; Venkatesh et al., 2003).

2.5 The insufficiency of adoption-oriented models

TAM and its extensions have generated a substantial body of knowledge on the drivers of initial adoption in Islamic digital banking (Davis, 1989; Venkatesh et al., 2003). Their prominence in the present corpus, 35.3 per cent of papers (12 of 34), reflects their parsimony and empirical tractability (Jamshidi, 2016; Parayil Iqbal, 2023; Suhartanto et al., 2022). However, these models treat trust as a positive, static antecedent to adoption and are structurally incapable of modelling what happens to that trust when the institutional relationship is disrupted by a security failure. PMT and Privacy Calculus model this trust-breach-recovery cycle more appropriately (Rogers, 1975, 1983; Dinev & Hart, 2006).

These three traditions belong together because each governs a different moment in the same trust relationship. *Maqasid al-Shariah* and *Amanah* define the institution's obligation to safeguard customer data; Protection Motivation Theory explains how a consumer appraises the threat when that obligation is tested; and Privacy Calculus explains how the disclosure decision is weighed in the first place. Adoption models address none of these critical moments in the trust relationship, underscoring the need for their integration.

2.6 Framing declaration

The Perceived *Amanah* Alignment construct and the Shariah non-compliance amplifier are not findings of this systematic review. They are conceptual lenses motivated by the theoretical gaps identified in the corpus and proposed here as directions for future theoretical development and empirical testing. Their presentation in this section is explicitly positioned as a research agenda contribution derived from the review rather than an output validated by it (Paul & Criado, 2020).

Note

Layer 1 feeds simultaneously into Layers 2 and 3; the Shariah non-compliance risk amplifier and Perceived Amanah Alignment are conceptual extensions derived from identified gaps, not empirical findings of the review. Hifz-Al-Aql is deliberately excluded as theologically contestable for information security.

3 METHODOLOGY

3.1 Research design and tool-to-RQ mapping

This review deploys a hybrid research design in which the choice of analytical tool is determined by the nature of each research question. Bibliometric performance analysis and science mapping address RQ1 and RQ2 respectively (Van Eck & Waltman, 2010, 2014). TCCM-coded systematic synthesis (Paul & Criado, 2020) addresses RQ3. The Research Agenda Matrix addresses RQ4 (Paul et al., 2021). The PRISMA 2020 reporting standard, the MMAT appraisal, the TCCM coding protocol, and the SPAR-4-SLR procedure operate as complementary, mutually reinforcing quality-assurance mechanisms spanning reporting, quality appraisal, synthesis, and review procedure.

3.2 SPAR-4-SLR protocol

The overarching methodological framework is the Scientific Procedures and Rationales for Systematic Literature Reviews (SPAR-4-SLR) protocol (Paul et al., 2021), which organises the review process into three auditable stages: Assembling (database retrieval and deduplication), Arranging (bibliometric mapping), and Assessing (TCCM-coded qualitative synthesis and derivation of the Research Agenda Matrix).

3.3 Search strategy and closed data horizon

Data were retrieved from the Scopus citation database, selected for its broad, consistent multidisciplinary coverage of peer-reviewed business, management, information-systems, and finance research relevant to this review. The search was executed using the following Boolean string applied to the TITLE-ABS-KEY field:

("Islamic bank" OR "Islamic fintech" OR "Islamic digital bank*" OR "sharia* bank*" OR "halal financ*") AND ("cybersecurity" OR "cyber security" OR "data privacy" OR "information security" OR "consumer trust" OR "digital trust" OR "privacy concern*" OR "data protection" OR "data breach*" OR "trust" OR "privacy" OR "security")*

The search was executed on 30 June 2025, and the temporal boundary was set from 1 January 2010 to 30 June 2025. The review applied a closed publication horizon of 30 June 2025: eligibility was restricted to studies published within the 1 January 2010 to 30 June 2025 window, and records published after 30 June 2025 were excluded, consistent with the SPAR-4-SLR protocol's requirement for a fixed and auditable dataset (Paul et al., 2021). Two records initially carried forward were subsequently confirmed to fall outside this window (published in September 2025) and were excluded, and are cited only as contextual literature. Studies published after this horizon represent an opportunity for future update reviews.

3.4 Tier separation declaration

Given the nascent size of the core corpus, a two-tier analytical design was adopted. Exploratory bibliometric mapping (performance analysis and title-term co-word mapping) was conducted on the full set of 200 identified records, designated Tier 1, to characterise the broader intellectual structure of the identified literature. The TCCM qualitative synthesis, MMAT appraisal, and all Islamic-specific thematic claims were confined strictly to the 34-paper peer-reviewed corpus, designated Tier 2. A dataset-architecture summary is provided in the supplementary material. This separation is maintained throughout Sections 4 to 7.

3.5 PRISMA 2020 flow

The corpus selection process, summarised in Fig. 2, followed the PRISMA 2020 reporting guidelines (Page et al., 2021). An automated duplicate check was performed using Mendeley; the resulting 200-record screening frame was retained for the inter-rater analysis. One exact duplicate was identified but retained, because both reviewers treated the two instances identically and the reliability analysis was defined on the supplied 200-record frame. Screening proceeded in two stages (Section 3.7). At the independent screening stage, under an inclusive dual-reviewer consensus rule in which a record was retained if either reviewer included it, 56 of the 200 records were excluded, both reviewers excluding, and 144 were retained. These 144 records were assessed for eligibility against the full study-level scope and document-type criteria in Table 2, and 110 were excluded, yielding a final corpus of 34 peer-reviewed journal articles and review papers that were individually retrieved, coded, and audited. Of the 110 eligibility-stage exclusions, eight are individually identifiable from the screening log and the venue metadata recorded there and are listed with their reasons in the supplementary Retrieval_Eligibility sheet: six on document type (four conference or symposium proceedings and two book chapters), one on substantive scope (a bibliometric review of artificial intelligence and machine learning in human-resource management), and one whose bibliographic details could not be independently verified. The remaining excluded records did not meet the full inclusion criteria on detailed assessment; because per-record eligibility flags for every intermediate record were not retained in the archived project files, these are retained as an aggregate stage count rather than individually reconstructed, a constraint stated as a limitation (Section 8.2). Separately, two Future Business Journal reviews published on 24 September 2025, after the closed 30 June 2025 horizon, were identified during peer review and are cited as contextual literature only; they are not part of the closed-horizon corpus. The reduction from 200 records

to 34 papers is consistent with the early stage of this research intersection. The full PRISMA 2020 twenty-seven-item checklist is provided as Supplementary Appendix B, and the criterion-level MMAT appraisals as Supplementary Appendix A.

Note

Records flagged as non-English at the screening stage are reported as excluded under the language criterion. The closed data horizon is 30 June 2025 (Page et al., 2021).

3.6 Inclusion and exclusion criteria

Table 2 documents the operational criteria applied at the screening and eligibility stages. The eligibility criteria were specified before the screening and eligibility assessment.

Table 2
Inclusion and exclusion criteria

Criterion	Inclusion	Exclusion
Topic scope	Papers primarily addressing consumer trust, data privacy, cybersecurity, or digital adoption with a security dimension within Islamic banking or Islamic FinTech	General Islamic banking performance, capital structure, Zakat, Waqf, Takaful, or service quality papers with no security or privacy construct
Document type	Peer-reviewed journal articles and review papers	Conference proceedings, book chapters, editorials, and grey literature
Language	English-language publications	Non-English publications (counted and reported in PRISMA flow as acknowledged limitation)
Time horizon	1 January 2010 to 30 June 2025 (inclusive)	Publications before January 2010 or after the closed horizon of 30 June 2025
Indexing	Actively indexed in Scopus at time of data collection	Records from unindexed sources or databases other than Scopus
Quality	Peer-reviewed journals indexed in Scopus, irrespective of quartile	Non-peer-reviewed sources, trade publications, and practitioner white papers

3.7 Screening and inter-rater reliability

Two of the authors independently screened all 200 retrieved records against the criteria in Table 2, using the bibliographic fields available in the export (principally title, authors, source, year, document type, and DOI). Cohen's Kappa was calculated to provide a formal inter-rater reliability metric for the independent screening decisions; the value obtained was $\kappa = 0.40$ (percentage agreement 70.5 per cent), corresponding to fair agreement on the benchmark scale of Landis and Koch (1977). Two of the authors screened from complementary disciplinary perspectives, one in marketing and consumer trust and the other in operations, information security, and Shariah governance, so disagreements clustered at the

boundaries of an interdisciplinary scope rather than reflecting random inconsistency. All 59 disagreements were resolved through structured discussion, with the resolution principle recorded for each case. Under the inclusive consensus rule (a record was retained if either reviewer included it), 144 of the 200 records were retained and 56 excluded at this independent-screening stage; these 144 records then underwent eligibility assessment against the full study-level scope and document-type criteria in Table 2, of which 110 were excluded, yielding the final corpus of 34 peer-reviewed journal articles and review papers. The archived materials permit individual identification of eight of these eligibility-stage exclusions (document type, substantive scope, or unverifiable record); the remainder are retained as an aggregate stage count because their record-level eligibility flags were not archived.

3.8 Quality appraisal via MMAT

All empirical papers in the corpus were appraised with the Mixed Methods Appraisal Tool (MMAT; Hong et al., 2018). Each empirical paper was assigned to its MMAT category and judged against the two screening questions and the five category-specific criteria (Yes, No, or Cannot tell), rather than being reduced to a single score; reviews, conceptual, and purely technical papers fall outside the MMAT empirical categories and are marked accordingly. Quality appraisal did not alter inclusion; it is used to qualify the interpretive weight given to each study in the synthesis. Criterion-level appraisals are provided in Supplementary Appendix A.

3.9 TCCM coding protocol

The qualitative synthesis followed the TCCM framework (Paul & Criado, 2020). Before full-scale coding commenced, a pilot exercise was conducted on ten randomly selected papers. Two of the authors coded the same ten papers independently, compared outputs, and resolved definitional disagreements to produce a shared codebook. The following example applies the TCCM framework to Parayil Iqbal (2023):

Theory

Extended UTAUT with institutional trust as a mediating variable; trust treated as a static positive antecedent to adoption intent.

Context

Islamic mobile banking consumers in the Maldives; legacy commercial banks; urban setting.

Characteristics

Cross-sectional survey; n = 312; convenience sample; no longitudinal tracking.

Methodology

partial least squares structural equation modelling (PLS-SEM) via SmartPLS; common method bias acknowledged but not corrected for.

A complete theory-coding audit table for all 34 papers, confirming the 0/34 PMT and Privacy Calculus findings, is provided as Supplementary Appendix C. All 34 papers were individually retrieved and independently coded by two of the authors, who reached consensus on the presence or absence of each focal framework; a separate reliability coefficient for the theory coding was not computed, and this is noted as a limitation in Section 8.2.

3.10 Science-mapping parameters and sensitivity analysis

Because the author and index keyword fields were not populated in the available Scopus export, the science mapping used a title-term co-occurrence (co-word) analysis rather than an author-keyword analysis, and is described as title-term co-occurrence throughout. Title terms from the 200 identified records were cleaned by lower-casing, removing search-defining terms (Islamic, bank, banking) and generic stop-words, and unifying obvious synonyms through a thesaurus; co-occurrence networks were built with association-strength normalisation (van Eck & Waltman, 2010, 2014). At a minimum occurrence threshold of five, 48 terms were retained, forming 322 co-occurrence links and five modularity-based clusters; threshold sensitivity was examined at 3, 5, and 8 (113, 48, and 25 terms, respectively), and the five-cluster solution reported here is based on the threshold of five. Callon centrality and density were then computed for each cluster to construct the strategic diagram in Fig. 4.

Co-citation and bibliographic-coupling analyses were not conducted, because the available metadata export did not contain cited-reference lists; the science mapping therefore rests on performance analysis and title-term co-occurrence, both of which are reproducible from the deposited data.

3.11 Database limitation

Scopus was selected as the single source database because it offers broad, consistent multidisciplinary coverage of peer-reviewed business, management, information-systems, and finance research relevant to this review, and because using a single, internally consistent database supports an auditable search and deduplication process. Prioritising a single, internally consistent database also avoids the record-matching and de-duplication artefacts that can arise when heterogeneous indices are merged. Extending coverage to Web of Science is identified as a valuable direction for future update reviews rather than a constraint on the present synthesis; this scope condition is revisited in Section 8.

4 RESULTS A: PERFORMANCE ANALYSIS

The performance analysis maps the bibliometric profile of the 34-paper corpus and interprets what the patterns imply for the field's development (RQ1; Paul et al., 2021).

4.1 Annual publication trajectory and inflection points

Annual publication counts are presented in Fig. 3. The field exhibits three distinct periods: 2013–2015 produced four papers, 2016–2020 produced nine papers, and 2021–2025 produced twenty-one papers, about three-fifths of the corpus; expressed as annual rates, output rose from roughly 1.3 papers per year

in the earliest period to about four per year in the most recent. The search window opened in January 2010; the earliest peer-reviewed record in the corpus appeared in 2013.

The modest uptick in 2020 coincides with the pandemic-driven acceleration of contactless and mobile banking adoption across Muslim-majority economies (Sudarsono et al., 2020). The sharper acceleration from 2022 onward coincides with increasing regulatory attention to cyber risk in Islamic banking institutions (IFSB, 2024) and with the rapid proliferation of native Islamic FinTech platforms across Southeast Asia and the Middle East (Idrees et al., 2024; Riza et al., 2024). A temporal term-frequency analysis (R-bibliometrix fieldByYear) indicates that terms associated with artificial intelligence, digital trust, and blockchain reached their highest frequencies in 2022 to 2025 (Ridzuan, 2024; Abdurrahman et al., 2024), while basic mobile-banking adoption terms were most frequent between 2016 and 2019 (Jamshidi, 2016; Mohd Thas Thaker et al., 2019); this is a descriptive trend analysis, not a formal citation-burst procedure. All annotations indicate coincidence rather than causation.

Note

About three-fifths of the corpus (21 of 34) appeared in 2021–2025. Coincidence annotations (no causation implied): the 2020 rise coincides with the COVID-19 shift to contactless and mobile banking; the 2022–2025 acceleration coincides with rising regulatory attention to cyber risk and the proliferation of native Islamic FinTech platforms.

4.2 Core outlets and concentration analysis

The 34 papers are distributed across 23 distinct journals. The Journal of Islamic Marketing contributes nine papers (26.5 per cent). Table 3 presents the five most productive journals. The concentration within a marketing journal coincides with the prevalence of consumer adoption frameworks and the near-total absence of cybersecurity-oriented theories (Davis, 1989; Morgan & Hunt, 1994). Future Business Journal contributes one corpus paper (Alsmadi, 2025); two further recent Future Business Journal reviews (Shahimi et al., 2025; Abakpa & Dvouletý, 2025) appeared in September 2025, after the June 2025 search horizon, and are discussed as contextual literature rather than as corpus items.

Table 3
Top journals by publication count and disciplinary orientation

Journal	Publisher	n	Disciplinary note
Journal of Islamic Marketing (Emerald)	Emerald	9 (26.5%)	Dominant outlet for Islamic consumer behaviour; explains the prevalence of adoption models (Jamshidi, 2016; Parayil Iqbal, 2023)
Intl J of Islamic and Middle Eastern Finance and Management	Emerald	2 (5.9%)	Adoption and governance (Irimia-Diéguez et al., 2024; Yaseen et al., 2022)
International Journal of Data and Network Science	Various	2 (5.9%)	Islamic FinTech acceptance and blockchain (Alnsour et al., 2023; Mbaidin et al., 2024)
Humanomics	Emerald	2 (5.9%)	Islamic economics and Maqasid applications (Shinkafi, 2017; Jamshidi & Hussin, 2016)
Future Business Journal (SpringerOpen)	Springer	1 (2.9%)	Target journal; Islamic FinTech and CSR adoption (Alsmadi, 2025)
All other journals (1 paper each)	Various	18 (52.9%)	Fragmented across 18 distinct outlets
<i>Note. Percentages calculated against the total corpus of 34 papers. The Future Business Journal corpus paper (Alsmadi, 2025) and the two contextual FBJ reviews (Shahimi et al., 2025; Abakpa & Dvouletý, 2025) address adjacent but non-overlapping dimensions of the field.</i>			

4.3 Geographic distribution and underrepresentation

Indonesia contributes the largest share with seven papers, followed by Jordan with five and Malaysia with three (Jamshidi, 2016; Parayil Iqbal, 2023; Mulia et al., 2021; Suhartanto et al., 2022; Mohd Thas Thaker et al., 2019). Pakistan contributes two papers (Haider et al., 2018; Ashraf et al., 2015), and the United Arab Emirates (Al Hammadi et al., 2024), the Maldives (Parayil Iqbal, 2023), and other national contexts one each. Bangladesh appears in one paper (Mazumder, 2022), the only paper in the corpus that directly engages with cybersecurity through an Islamic banking institutional lens. Many of the remaining papers use cross-national survey panels or do not specify a country context (Naeem, 2021; Suhartanto et al., 2022), making it impossible to determine whether their findings generalise to the South Asian and sub-Saharan African markets where Islamic banking is growing most rapidly.

4.4 Author productivity and fragmentation

The most productive authors, D. Jamshidi and M. Naeem, each contribute two papers (Jamshidi, 2016; Jamshidi & Hussin, 2016; Naeem, 2019, 2021). No author reaches three publications on this specific intersection. This flat productivity distribution suggests that the field has not yet attracted a cohesive research community with a sustained programme of inquiry into cybersecurity and trust in Islamic digital banking.

4.5 Citation impact and intellectual anchors

Table 4 presents the five most cited papers in the corpus as at 30 June 2025.

Table 4
Five most cited papers in the corpus: intellectual contribution

Study	Cites	Primary construct	Intellectual contribution
Ridzuan (2024) DOI: 10.3390/info15080432	90	AI, regulation, and ethics in financial services	Signals comparatively strong recent scholarly attention to AI governance and ethics in financial services
Jamshidi (2016) DOI: 10.1108/JIMA-07-2014-0050	73	TAM extended with religiosity and trust	Anchors the dominant TAM-with-religious-variable paradigm; adoption without security constructs
Shinkafi (2017) DOI: 10.1108/H-03-2017-0041	51	<i>Maqasid al-Shariah</i> in Islamic economics	Most cited explicitly Islamic theoretical paper; normative grounding for this review's Layer 1
Ashraf et al. (2015) DOI: 10.1057/fsm.2015.8	48	Consumer trust and compliance confidence	Related qualitative evidence informing the proposed Perceived Amanah Alignment construct; not a direct validation
Parayil Iqbal (2023) DOI: 10.1108/JIMA-01-2022-0030	39	Extended UTAUT with institutional trust	Trust variables carry explanatory weight independent of utility constructs; TCCM worked example in Section 3.9

Note. Citation counts were retrieved from Google Scholar on 30 June 2025 and are indicative only; they fluctuate over time and are not Scopus counts. All DOIs were verified.

Three observations emerge. First, Ridzuan (2024) records a comparatively high indicative Google Scholar citation count within the corpus; because it is a recent conceptual paper, this count should be read with caution as a tentative rather than definitive signal of interest at the AI-ethics-Islamic finance nexus. Second, Shinkafi (2017) remains the most cited explicitly Islamic theoretical paper, indicating that *Maqasid al-Shariah* retains its standing as the preferred normative anchor despite its limited application to digital security contexts. Third, the absence of any cybersecurity-specific paper in the top five citation rankings provides a further quantitative dimension to the gap identified qualitatively through the TCCM synthesis (Ashraf et al., 2015).

4.6 Document type distribution

All 34 papers in the final corpus are peer-reviewed journal articles, review papers, or conceptual articles. Of these, six are review, conceptual, or technical papers and 28 are empirical studies. The presence of only six review, conceptual, or technical papers over roughly a decade is consistent with the gap that the present review addresses, namely that systematic synthesis has not kept pace with knowledge production (Paul & Criado, 2020).

5 RESULTS B: SCIENCE MAPPING

This section addresses RQ2 by analysing the intellectual structure of the identified literature through a title-term co-occurrence (co-word) analysis and a thematic (strategic) diagram. Consistent with an emerging research domain, the resulting networks are relatively sparse. This sparsity is anticipated and is itself an informative finding: it visually confirms that the intersection of cybersecurity, data privacy, and consumer trust in Islamic digital banking has not yet generated the dense bibliometric co-occurrence structures that characterise mature fields (Van Eck & Waltman, 2014). All analyses were conducted with fractional counting and association strength normalisation applied.

5.1 Title-term co-occurrence analysis and thematic cluster architecture

The title-term co-occurrence analysis identifies five modularity-based clusters, summarised in Table 5. Each cluster is labelled using theoretical language rather than default numeric labels (Van Eck & Waltman, 2010), and cluster size is expressed as the number of constituent title terms rather than as a share of the corpus.

Table 5

Science mapping cluster architecture: composition, frameworks, contexts, and structural blind spots

Cluster	Terms (n)	Leading title terms	Interpretation	Structural blind spot
C1: Relationship trust & loyalty	14	customer, trust, loyalty, service, satisfaction	Relational trust, loyalty and satisfaction; central in the network.	Trust treated as a static antecedent; no breach or recovery dynamics.
C2: Technology adoption & intention	12	adoption, malaysia, social, finance, performance	Adoption intention and mobile-banking use; motor/basic theme.	Adoption under stable conditions; no threat appraisal.
C3: FinTech, blockchain & technology	10	financial, blockchain, industry, management, through	Emerging technologies (blockchain, AI) in Islamic finance.	Technology capability without consumer security or privacy analysis.
C4: Shariah governance & compliance	8	countries, governance, disclosure, corporate, gcc	Shariah governance, disclosure and regulation; dense niche theme.	Governance oriented to asset compliance; data protection absent.
C5: Islamic-finance performance & FinTech	4	sector, data, compliance, consumer	Islamic-finance performance and FinTech context (Malaysia-centred).	Performance/adoption focus; security and privacy peripheral.
<i>Note. Clusters are modularity-based communities of the title-term co-occurrence network computed on the 200 identified records (Section 3.10). Cluster size is the number of constituent title terms; leading terms are the highest-frequency members. Minimum occurrence threshold five; association-strength normalisation (Van Eck & Waltman, 2014).</i>				

The two largest clusters are organised around relationship trust (customer, trust, loyalty, service, satisfaction) and technology adoption (adoption, intention, mobile). Both occupy relatively central positions in the co-word network, consistent with the field's orientation toward adoption and relational trust; their shared structural blind spot is that trust is treated as a positive antecedent under stable conditions, with no analysis of trust dynamics under cybersecurity threat or following institutional breach (Jamshidi, 2016; Mulia et al., 2021; Suhartanto et al., 2022; Mohd Thas Thaker et al., 2019).

A further cluster is organised around emerging technologies (financial, blockchain, technology, management), reflecting recent work on blockchain, artificial intelligence, and Islamic FinTech (Unal, 2022; Mbaidin et al., 2024; Abdurrahman et al., 2024). Its blind spot is the examination of technology capabilities without corresponding investigation of consumer security anxieties or data privacy trade-offs.

A governance cluster (governance, compliance, disclosure, regulatory) occupies a dense but less central, niche position and encompasses Shariah governance, regulation, and Maqasid al-Shariah as a normative reference point (Shinkafi, 2017; Alkhamees, 2013; Alsmadi, 2015). Although closest in orientation to this review's Layer 1 anchor, it contains no papers connecting governance obligations to data protection, cybersecurity mandates, or consumer privacy implications.

The remaining terms group into an Islamic-finance performance and FinTech context (Malaysia, performance, finance, fintech, financing) and a small set of security- and privacy-oriented terms that remain peripheral in the network. Security and privacy terms have low centrality, reflecting their marginal position within the field's current intellectual structure (Khan & Alibrahim, 2023; Hamsin et al., 2023; Mazumder, 2022; Ashraf et al., 2015). This peripheral position, measuring trust outcomes without examining the security mechanisms through which trust is violated, is the most direct motivation for the three-layer framework proposed in Section 2.

5.2 Thematic structure and strategic diagram

Figure 4 presents the strategic (thematic) diagram, plotting each title-term cluster by Callon centrality (external association strength) and density (internal association strength), computed from the co-word network described in Section 3.10. Quadrant boundaries are set at the median centrality and density across clusters.

Note

Cluster positions are computed Callon centrality and density values from the title-term co-word network (Section 3.10); axes are median-split into motor, basic, niche, and emerging quadrants; bubble area is proportional to the number of constituent title terms. The computed centrality and density values for each cluster are reported in the supplementary Master corpus file (Coword_Clusters sheet); the median lines are retained as a visual reference rather than a substantive threshold, and any cluster lying close to a median is interpreted with corresponding caution.

In the computed diagram, the relationship-trust and technology-adoption clusters occupy high-centrality positions consistent with basic and motor themes, the governance cluster sits in a high-density, lower-centrality niche position, and the security- and technology-oriented terms remain comparatively peripheral. This positioning is consistent with a security research frontier that is emerging but not yet central to the field (Van Eck & Waltman, 2014).

6 RESULTS C: TCCM SYNTHESIS

This section addresses RQ3 by applying the TCCM framework (Paul & Criado, 2020) to the 34-paper peer-reviewed corpus. All analyses and interpretive claims are confined to Tier 2, the peer-reviewed corpus, in accordance with the tier separation declaration in Section 3.4. Throughout this section, a deliberate tone discipline is maintained: where the identified corpus does not include certain theoretical

frameworks or methodological approaches, this is reported as an empirical characteristic of the literature rather than a normative failure.

6.1 Theoretical directives

The theory distribution across the 34-paper corpus is presented in Table 6. Three patterns define the theoretical profile of the corpus: a pronounced concentration in adoption-oriented frameworks, a near-total absence of cybersecurity-specific theories, and the absence of any integrated Islamic ethics and security model.

Table 6
Distribution of focal theoretical frameworks in the 34-paper corpus

Theoretical framework	Papers (n = 34)	Share	Role and interpretive note
TAM and UTAUT variants	12	35.3%	Adoption intention; trust as static antecedent (Davis, 1989; Venkatesh et al., 2003; Jamshidi, 2016; Parayil Iqbal, 2023)
Relationship marketing trust models	7	20.6%	Trust as relational outcome; no breach dimension (Morgan & Hunt, 1994; Mayer et al., 1995; Ashraf et al., 2015; Sumaedi et al., 2015)
Shariah governance frameworks	4	11.8%	Regulatory and board governance; asset compliance orientation (Alkhamees, 2013; Mbaidin et al., 2024)
<i>Maqasid al-Shariah</i> (normative only)	1	2.9%	Normative philosophical reference only; never operationalised with cybersecurity or privacy (Shinkafi, 2017)
Protection Motivation Theory (PMT)	0	0.0%	Absent from all 34 papers. PMT is among the frameworks most frequently applied in information-security research (Sommestad et al., 2015; Rogers, 1975, 1983). Its absence is a structural characteristic of this corpus.
Privacy Calculus Theory	0	0.0%	Absent from all 34 papers. Privacy Calculus is among the widely used models of privacy decision-making in digital services research (Dinev & Hart, 2006). Its absence is equally noteworthy.
Integrated <i>Maqasid</i> -security or <i>Maqasid</i> -privacy framework	0	0.0%	Absent from all 34 papers. <i>No paper connects Maqasid al-Shariah to cybersecurity governance, data privacy obligations, or consumer digital trust in any operational form.</i>
<i>Note. Frameworks shown in bold, each with a 0.0 per cent share, are absent from the identified corpus despite their established presence in adjacent research domains. The four named framework rows account for 24 of the 34 papers; the remaining 10 papers (29.4 per cent) use heterogeneous other frameworks or no single named behavioural theory (reviews, conceptual, technical, or descriptive studies).</i>			

Theory classification conducted through TCCM coding by two of the authors independently (Paul & Criado, 2020); the two coders independently assessed the presence or absence of each focal framework, Protection Motivation Theory, Privacy Calculus, and integrated Maqasid–security models, and resolved any differences by consensus across all 34 papers, following pilot calibration on ten papers; no separate reliability coefficient was computed. Full coding audit is provided in Supplementary Appendix C.

TAM and UTAUT variants appear in 35.3 per cent of papers (Davis, 1989; Venkatesh et al., 2003; Jamshidi, 2016; Parayil Iqbal, 2023; Suhartanto et al., 2022; Haider et al., 2018), establishing adoption modelling as the dominant theoretical paradigm. Relationship marketing trust models account for a further 20.6 per cent (Morgan & Hunt, 1994; Mayer et al., 1995; Ashraf et al., 2015; Sumaedi et al., 2015), in which trust is predominantly treated as a positive baseline predictor of continued engagement rather than a construct whose dynamics under institutional failure warrant investigation.

The three rows at the bottom of Table 6 constitute the section's key findings. Protection Motivation Theory does not appear in any of the 34 papers. Given that PMT is among the frameworks most frequently applied in information-security research, as synthesised by Sommestad et al. (2015) (Rogers, 1975, 1983), its absence from the identified Islamic digital banking corpus is a characteristic of the literature reviewed rather than a sampling coincidence. Privacy Calculus Theory (Dinev & Hart, 2006) is similarly absent from all 34 papers, despite being among the most widely applied models of privacy decision-making in digital services research. No paper in the corpus connects *Maqasid al-Shariah* to cybersecurity governance, data privacy obligations, or digital consumer trust in any operational or empirically testable sense (Shinkafi, 2017).

An alternative reading is that such frameworks are present implicitly but were not labelled as such by the original authors. However, because coding applied explicit, pre-specified operational definitions and the two coders reached consensus on the presence or absence of these focal frameworks, systematic omission is the more plausible interpretation than implicit, unlabelled use (Supplementary Appendix C).

Expressed as a coding matrix, the cell intersecting Protection Motivation Theory, or Privacy Calculus, with the Islamic digital banking context records a count of zero across all 34 papers.

6.2 Contextual boundaries

The corpus exhibits pronounced geographic and institutional concentration. Indonesia (seven papers) and Jordan (five) are the most represented national contexts, followed by Malaysia (three) (Jamshidi, 2016; Parayil Iqbal, 2023; Mulia et al., 2021; Suhartanto et al., 2022; Mohd Thas Thaker et al., 2019). Among Gulf Cooperation Council settings, only the United Arab Emirates appears (Al Hammadi et al., 2024); Yaseen et al. (2022) and Mbaidin et al. (2024) are set in Jordan, which is not a GCC member. Bangladesh appears in one paper (Mazumder, 2022), the only paper in the corpus to engage directly with cybersecurity through an Islamic banking institutional frame. Many of the remaining papers use cross-national panels or do not specify a national context (Naeem, 2021; Suhartanto et al., 2022), making it

impossible to assess whether their findings are generalisable to South Asian and sub-Saharan African markets.

The institutional distinction between legacy Islamic commercial banks and native Islamic FinTech platforms is rarely observed in the corpus. Twenty of the 34 papers study legacy Islamic banks and five focus on native Islamic FinTech platforms, with two hybrid cases; the remaining papers are conceptual, technical, or review studies (Dawood et al., 2022; Idrees et al., 2024; Unal, 2022). Classification criteria and the per-paper institutional category are reported in Supplementary Appendix C. The cybersecurity implications of this distinction are substantial: legacy banks operate established Shariah Supervisory Boards oriented toward asset and transaction compliance, whereas native FinTech platforms are typically more agile but lack equivalent institutionalised Shariah governance tuned to data processing, a divergence the existing literature has yet to characterise.

6.3 Study characteristics

The empirical design of the corpus is strikingly homogeneous. Nineteen of the 34 papers, about 68 per cent of the 28 empirical studies, employ cross-sectional quantitative designs, predominantly survey-based and analysed with PLS-SEM or regression (Jamshidi, 2016; Parayil Iqbal, 2023; Mansour et al., 2016; Haider et al., 2018; Sumaedi et al., 2015; Mulia et al., 2021; Naeem, 2021; Ashurov et al., 2019). Most significantly, we identified no longitudinal empirical studies among the final eligible corpus. The empirical consumer studies are predominantly cross-sectional, measuring consumer trust at a single point in time under the implicit assumption that institutional conditions are stable. There are no studies in the corpus that track trust dynamics before, during, and after a security incident (Mazumder, 2022 is a partial exception, examining post-heist disclosure patterns).

6.4 Methodological imperatives

MMAT quality appraisal (Hong et al., 2018) suggests that the corpus exhibits a pattern of replication rather than methodological innovation. The overwhelming reliance on PLS-SEM survey designs has generated a body of knowledge that is internally coherent but narrow in its evidentiary base. The methodological toolkit has not evolved meaningfully since approximately 2015. Qualitative, computational, and technical or experimental designs remain a minority of the corpus, for example, machine-learning risk analysis (Aysan et al., 2024), textual/NLP analysis of cyber-risk disclosure (Mazumder, 2022), and biometric security evaluation (Khan & Alibrahim, 2023), and no longitudinal empirical study of consumer trust dynamics was identified. These boundaries define the methodological frontier and are reflected in the varied research designs specified for Propositions 1 through 6 in Section 7.

6.5 Synthesis: answering RQ3

The TCCM analysis (Paul & Criado, 2020) generates a clear and empirically grounded answer to RQ3. Islamic ethical frameworks, *Amanah*, *Hifz al-Mal*, and *Maqasid al-Shariah*, are present in the identified corpus almost exclusively as philosophical background or adoption-facilitating variables (Shinkafi, 2017;

Alkhamees, 2013; Alsmadi, 2015). They appear as rhetorical anchors that lend Islamic legitimacy to standard adoption frameworks rather than as operational constructs that modify how trust, privacy, or cybersecurity are theorised. Western behavioural models of security risk, principally PMT (Rogers, 1975, 1983) and Privacy Calculus (Dinev & Hart, 2006), are not represented in the corpus. The two paradigms, Islamic ethics and cybersecurity psychology, have developed as parallel and non-intersecting literature streams within the identified corpus. The corpus has studied whether Muslim consumers trust Islamic digital banks (Ashraf et al., 2015; Mulia et al., 2021; Parayil Iqbal, 2023). It has not studied what happens to that trust when an institution fails its *Amanah* obligation through a data breach (Mazumder, 2022), nor has it modelled the cognitive and economic mechanisms through which Islamic consumers appraise and respond to cybersecurity threats. This separation is not a marginal gap at the edges of an otherwise developed field; it is a prominent open question within the identified corpus. These convergent gaps motivate the six testable propositions presented in Section 7, and the three-layer framework developed in Section 2 follows directly from them.

7 DISCUSSION: RESEARCH AGENDA AND PRACTICAL IMPLICATIONS

7.1 Synthesising the evidence base

Across three complementary analytical stages, a consistent pattern emerges. Scholarly production is accelerating, with about three-fifths of the corpus appearing in 2021 to 2025 (Section 4); the field remains organised around digital adoption and governance frameworks that treat trust as a static construct immune to cybersecurity disruption (Section 5); and Protection Motivation Theory, Privacy Calculus, and any operational integration of Maqasid al-Shariah with security or privacy models are absent from all 34 papers in the identified corpus (Section 6).

These findings are not incidental lacunae at the margins of an otherwise developed field; they represent its central unaddressed question. The *Amanah* duty to protect consumer data, as a form of protected property under *Hifz al-Mal* (Shinkafi, 2017), has never been operationalised in connection with the psychological and economic frameworks that explain how consumers actually respond to cybersecurity threats. Consistent with the framing declaration in Section 2.6, the Shariah non-compliance risk amplifier and Perceived *Amanah* Alignment are presented in the propositions below as directions for future empirical testing rather than as validated findings of this review (Paul & Criado, 2020). Each proposition is traceable to a specific corpus observation and specifies a method that departs from the cross-sectional survey design dominating the empirical studies (about 68 per cent of empirical studies; Section 6.3). Although the reviewed studies are geographically concentrated, the propositions are pitched at a level of abstraction that permits testing across diverse Islamic banking systems, and the framework represents one synthesis consistent with the reviewed evidence rather than a definitive account.

7.2 Research agenda matrix

Table 7 presents the Research Agenda Matrix, mapping six testable propositions to the theoretical gaps identified in the preceding sections, together with the theoretical lens, recommended method, and target context for each proposition.

Table 7
Research Agenda Matrix: six testable propositions across four thematic gaps

P1	Gap and source	Testable proposition	Theoretical lens	Recommended method	Target context
	PMT absent (§ 6.1: 0/34)	In Islamic digital banking, perceived Shariah non-compliance risk amplifies the threat-appraisal pathway, significantly moderating the relationship between a perceived security vulnerability and the velocity of consumer trust withdrawal.	PMT (Rogers, 1975, 1983) with Shariah amplifier; threat and coping appraisal pathways	Multi-country longitudinal survey (two time points); PLS-SEM with moderation analysis	Malaysia, Indonesia
P2	Privacy Calculus and Perceived Amanah Alignment absent (§ 6.1: 0/34)	Islamic religiosity moderates the digital privacy cost-benefit calculation such that high-religiosity consumers assign greater weight to Perceived Amanah Alignment as a non-monetary spiritual benefit.	Privacy Calculus (Dinev & Hart, 2006) with Perceived Amanah Alignment; religiosity as moderator	Choice-based experimental conjoint analysis; religiosity as between-subjects factor	Pakistan, Bangladesh
P3	Shariah board cybersecurity role absent (§ 6.2 and § 6.3: no breach-recovery studies; zero longitudinal designs)	Following an institutional data breach, transparency disclosures authenticated by a Shariah Supervisory Board yield a significantly steeper trust-recovery trajectory than identical disclosures issued by a conventional	Institutional Trust Theory and Institutional Amanah; expectation-violation effect (Grégoire et al., 2009)	Scenario-based longitudinal vignette experiment; trust at three points, pre-breach, post-breach, post-disclosure	GCC, Malaysia

Note. Each proposition is derived from and traceable to specific corpus findings, cited by section. The Shariah non-compliance risk amplifier (P1, P3) and Perceived Amanah Alignment (P2, P6) are proposed as conceptual lenses for future empirical testing; they are not findings of this review. Research methods are specified to diversify beyond the cross-sectional survey designs that dominate the empirical studies (Hong et al., 2018). The propositions are theory-derived conjectures for future testing, not findings of this review.

		corporate compliance committee, mitigating the expectation-violation effect.			
P4	Regulatory intersection absent (§ 6.2: no paper crosses national data law with IFSB cybersecurity standards)	P4a: Greater divergence between national data-protection requirements and IFSB cybersecurity guidance is associated with greater perceived regulatory ambiguity among Islamic financial institutions. P4b: Greater perceived regulatory ambiguity is, in turn, associated with higher consumer perceived cybersecurity risk.	Institutional Theory (DiMaggio & Powell, 1983); regulatory isomorphism	Comparative regulatory case study combined with a consumer perceived-risk survey across three jurisdictions	Malaysia, Saudi Arabia, Bangladesh
P5	Legacy bank vs. native FinTech absent (§ 6.2: 20/34 legacy banks; 5/34 native FinTech)	Native Islamic FinTech platforms may experience faster consumer trust recovery following a cybersecurity incident than legacy Islamic banks, because trust is anchored in product performance and Shariah transparency rather than relational inertia. Here, faster recovery denotes a steeper slope of consumer trust recovery between the post-breach	Trust Transfer Theory (Stewart, 2003); post-breach recovery trajectories	Longitudinal, pre/post-incident mixed-methods design: repeated consumer surveys combined with in-depth executive interviews	UAE, United Kingdom
<i>Note. Each proposition is derived from and traceable to specific corpus findings, cited by section. The Shariah non-compliance risk amplifier (P1, P3) and Perceived Amanah Alignment (P2, P6) are proposed as conceptual lenses for future empirical testing; they are not findings of this review. Research methods are specified to diversify beyond the cross-sectional survey designs that dominate the empirical studies (Hong et al., 2018). The propositions are theory-derived conjectures for future testing, not findings of this review.</i>					

		and follow-up measurements.			
P6	South Asia underrepresented; longitudinal consumer-trust designs absent (§ 6.2; § 6.3: no longitudinal empirical studies of consumer trust; Mazumder, 2022 the sole Bangladesh paper)	Consumer discourse following actual digital banking disruptions in South Asian Islamic institutions reveals trust and privacy anxieties not captured by survey instruments designed for Malaysian and Indonesian contexts.	PMT and Perceived Amanah Alignment in South Asian cultural context; grounded theory	Qualitative netnography and structural topic modelling of real consumer complaint texts following documented digital disruption events	Bangladesh, Pakistan
<i>Note. Each proposition is derived from and traceable to specific corpus findings, cited by section. The Shariah non-compliance risk amplifier (P1, P3) and Perceived Amanah Alignment (P2, P6) are proposed as conceptual lenses for future empirical testing; they are not findings of this review. Research methods are specified to diversify beyond the cross-sectional survey designs that dominate the empirical studies (Hong et al., 2018). The propositions are theory-derived conjectures for future testing, not findings of this review.</i>					

7.3 Practical and policy implications

For Chief Information Security Officers and senior management of Islamic banks, the central implication is one of strategic reframing. The three-layer framework reconstitutes data protection as a Shariah governance obligation embedded in the institution's *Amanah* covenant (Shinkafi, 2017). A data breach attributable to systemic negligence is therefore not only a financial and reputational risk; it may, depending on jurisdiction and governance arrangements, warrant consideration of notification to the institution's Shariah Supervisory Board alongside conventional regulatory reporting; this is offered as a policy option for investigation rather than an established requirement. Framing cybersecurity expenditure through this lens, as the operationalisation of *Hifz al-Mal* obligations, may be more effective in securing board-level commitment than conventional cost-benefit analyses (IFSB, 2024).

For marketing and corporate communications teams, the Perceived *Amanah* Alignment construct proposed in Section 2.4 suggests that when consumers perceive that an Islamic bank is actively fulfilling its *Amanah* duty, through independently verified security certifications, transparent privacy governance disclosures, and proactive communication of data protection practices, this perception may function as a non-monetary spiritual benefit that offsets privacy costs in the consumer's decision calculus (Ashraf et al., 2015; Dinev & Hart, 2006). Marketing communication that explicitly connects security investments to Shariah governance commitments has the potential to convert an institutional cost into a source of competitive differentiation among digitally engaged Muslim consumers.

For regulators and international standard-setting bodies, including the IFSB, Bank Negara Malaysia, the Saudi Central Bank, and Bangladesh Bank, the most pressing implication concerns the regulatory treatment of data breaches in Shariah-supervised financial institutions. Proposition 4 in Table 7 identifies a gap between national data protection statutes and IFSB cybersecurity guidance that the existing literature has not examined (DiMaggio & Powell, 1983). An integrated regulatory framework that treats a material data breach at an Islamic bank as both a conventional regulatory violation and a potential Shariah non-compliance event, under which a material data breach might trigger parallel consideration by the institution's Shariah Supervisory Board, the relevant monetary authority, and affected consumers, could help establish a governance architecture consistent with the Amanah obligations that define the sector's ethical foundations (Alkhamees, 2013; Mazumder, 2022; IFSB, 2024).

8 CONCLUSIONS

Research on consumer trust, data privacy, and cybersecurity in Islamic digital banking is expanding rapidly yet remains theoretically fragmented: output is growing, but the frameworks that explain how consumers appraise security threats and privacy trade-offs are not represented in the corpus.

RQ1 asked how scholarly production on consumer trust, data privacy, and emerging cybersecurity in Islamic digital banking has evolved. The 34-paper corpus shows a marked increase from the first to the third study period, with about three-fifths of the corpus appearing between 2021 and 2025. The field is anchored in the Journal of Islamic Marketing and concentrated particularly in Indonesian and Jordanian research contexts, with Malaysia also represented (Jamshidi, 2016; Parayil Iqbal, 2023). Growth coincides with the post-pandemic acceleration of contactless banking (Sudarsono et al., 2020) and with increasing regulatory attention to cyber risk in Islamic financial institutions (IFSB, 2024). South Asia remains severely underrepresented, with Bangladesh appearing in only one paper (Mazumder, 2022) despite housing one of the world's largest Islamic banking consumer populations.

RQ2 asked what intellectual pillars, thematic clusters, and research fronts shape the current discourse. The title-term co-word analysis identifies five thematic clusters, dominated by technology-adoption and relationship-trust terms, with governance, emerging-technology, and security- and privacy-oriented terms forming smaller groupings; in the strategic diagram, security and privacy terms remain peripheral (Davis, 1989; Venkatesh et al., 2003; Shinkafi, 2017; Ashraf et al., 2015; Khan & Alibrahim, 2023).

RQ3 asked how Islamic ethical frameworks currently integrate with Western behavioural trust and privacy models. The TCCM synthesis (Paul & Criado, 2020) establishes that *Maqasid al-Shariah* and *Amanah* appear in the identified corpus almost exclusively as philosophical background, never operationalised in connection with cybersecurity or data privacy constructs (Shinkafi, 2017). Protection Motivation Theory (Rogers, 1975, 1983) and Privacy Calculus Theory (Dinev & Hart, 2006) are absent from all 34 papers in the identified corpus. The two paradigms, Islamic ethics and cybersecurity psychology, have developed as parallel and non-intersecting literature streams within the identified corpus.

RQ4 asked what multi-disciplinary framework and testable propositions can guide future inquiry. Drawing on the synthesis, this review develops a three-layer conceptual framework in which *Maqasid al-Shariah* and *Amanah* serve as a shared normative anchor feeding simultaneously into Protection Motivation Theory (Rogers, 1975, 1983), extended with a Shariah non-compliance risk amplifier, and into Privacy Calculus Theory (Dinev & Hart, 2006), extended with Perceived *Amanah* Alignment as a spiritual benefit construct, informed by the related evidence of Ashraf et al. (2015) and the expectation-violation literature of Grégoire et al. (2009). Six testable propositions address the PMT gap, the Privacy Calculus gap, the absence of Shariah board governance in cybersecurity research, the regulatory intersection, the legacy bank versus Islamic FinTech distinction, and the underrepresentation of South Asian Islamic banking contexts (DiMaggio & Powell, 1983; Stewart, 2003).

8.1 Theoretical and practical contributions

This review makes two connected contributions. Theoretically, to the best of our knowledge, it is among the first to map the intellectual structure of the cybersecurity and digital trust domain within Islamic banking through a hybrid bibliometric and systematic method (Paul et al., 2021; Van Eck & Waltman, 2010), and to propose the integration of *Maqasid al-Shariah* with Protection Motivation Theory (Rogers, 1975, 1983) and Privacy Calculus (Dinev & Hart, 2006) as a framework for future empirical inquiry. The extension of the expectation-violation effect (Grégoire et al., 2009) into an Islamic jurisprudential context, framing a data breach as the transformation of an *Amanah* compliance asset into a non-compliance liability, offers a conceptual bridge between Islamic finance ethics and behavioural cybersecurity psychology that the existing literature has not attempted. Practically, the framework provides Islamic bank executives with a rationale for treating data protection as a Shariah governance obligation (IFSB, 2024; Alkhamees, 2013), marketing teams with a construct, Perceived *Amanah* Alignment, through which security transparency can be communicated as an ethical brand signal (Ashraf et al., 2015), and regulators with a policy direction for integrating data breach notification with Shariah Supervisory Board governance protocols (Mazumder, 2022).

8.2 Limitations

This review is subject to several limitations that bound the strength of its claims. First, data were retrieved from a single subscription database, Scopus, identified through a Publish-or-Perish export; incorporating Web of Science in future update reviews would assess cross-database coverage. Second, the search was restricted to English-language publications, which may under-represent Arabic and regional scholarship on *Maqasid al-Shariah* applications to digital finance, a limitation that Proposition 6 addresses. Third, the closed data horizon of 30 June 2025 excludes later work. Fourth, the exported metadata did not populate author or index keyword fields, so the science mapping used title terms rather than author keywords; a title-term co-occurrence network approximates, but is not equivalent to, an author-keyword co-occurrence network. Fifth, because the export did not contain cited-reference lists, co-citation and bibliographic-coupling analyses were not conducted, and the intellectual-structure findings rest on performance analysis and title-term co-occurrence. Sixth, screening reliability was fair

(Cohen's kappa = 0.40); this reflects the interdisciplinary breadth of the eligibility boundary, and all disagreements were resolved by consensus before the final corpus was fixed, but the coefficient is modest and the final inclusion decisions should be read in that light. Seventh, the review reports a two-stage screening funnel (200 records identified; 56 excluded by both reviewers; 144 assessed for eligibility; 110 excluded; 34 included), but per-record eligibility flags were not retained for every intermediate record; eight of the eligibility-stage exclusions are individually identifiable in the supplementary materials and the remainder are reconciled by stage and count, so the record-level detail of the intermediate exclusions cannot be fully reconstructed. Eighth, the citation counts in Table 4 are indicative Google Scholar values rather than Scopus counts. Finally, the corpus of 34 papers, though consistent with a nascent intersection, is small, and the absence findings are bounded to this identified Scopus corpus rather than to the field as a whole. Each limitation defines an empirical boundary that motivates one or more of the propositions in the Research Agenda Matrix.

Beyond these boundaries, the contribution of this review is to reframe consumer data protection in Islamic digital banking as an expression of the institution's *Amanah* obligation and to translate that reframing into a testable, theory-driven agenda. For researchers, it specifies where the next advances lie; for Islamic banks and FinTech providers, it links security investment to Shariah-governance commitments; and for regulators, it motivates an integrated treatment of data-breach and Shariah-compliance oversight. Pursuing these questions would move the field from documenting adoption towards safeguarding the trust on which Islamic digital finance ultimately depends.

Abbreviations

AI	artificial intelligence
FBJ	Future Business Journal
GCC	Gulf Cooperation Council
IFSB	Islamic Financial Services Board
MMAT	Mixed Methods Appraisal Tool
PLS-SEM	partial least squares structural equation modelling
PMT	Protection Motivation Theory
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RQ	research question

SPAR-4-SLR

Scientific Procedures and Rationales for Systematic Literature Reviews

TAM

Technology Acceptance Model

TCCM

Theory, Context, Characteristics, Methodology

UTAUT

Unified Theory of Acceptance and Use of Technology.

Declarations

Author Contribution

F.Z.S. led the conceptualisation of the study, contributed consumer-trust, marketing, and bibliometric expertise, conducted the bibliometric and science-mapping analyses, served as one of the two independent screeners and theory coders, and drafted the manuscript. N.H.I.C. contributed Islamic digital banking, cybersecurity, and Shariah-governance expertise, co-designed the methodology, served as the second independent screener and theory coder, and undertook critical review and editing. A.A.H. carried out the literature search and data curation, prepared and formatted the manuscript, and contributed to shaping its overall structure and revision. All authors read and approved the final manuscript.

Data Availability

The primary dataset was retrieved from the Scopus citation database, which is publicly accessible. The complete Boolean search string, inclusion and exclusion criteria, and PRISMA flow are documented in Section 3 to ensure full reproducibility. The Theory Coding Audit Table is provided as Supplementary Appendix C.

References

1. A
2. Abakpa, G. E., & Dvoutely, O. (2025). How does digitalisation shape business financial performance? A systematic literature review. *Future Business Journal*, 11(1), 235. <https://doi.org/10.1186/s43093-025-00659-8>
3. Abdurrahman, A., Sakti, A., Faruq, M., & Ardiansyah, R. (2024). Investigating the impact of digital business ecosystem in enhancing Islamic mobile banking performance. *Digital Business*, 4(2), 100096. <https://doi.org/10.1016/j.digbus.2024.100096>
4. Al Hammadi, M., Al-Sartawi, A. M. A. M., & Hamdan, A. (2024). Risk management in Islamic banking: The impact of financial technologies. *Risks*, 12(2), 17. <https://doi.org/10.3390/risks12020017>

5. Al-Afeef, M. (2024). Nurturing trust in Islamic banking within the metaverse for marketing. *Journal of Islamic Marketing*, 15(8), 2012–2034. <https://doi.org/10.1108/JIMA-01-2024-0040>
6. Alkhamees, A. (2013). The impact of Shari'ah governance practices on Shari'ah compliance in contemporary Islamic finance. *Journal of Banking Regulation*, 14(2), 134–163. <https://doi.org/10.1057/jbr.2012.12>
7. Alnsour, I., Alghadi, M., Ahmad, A., Alibraheem, M., Altahat, S., Al-Smadi, R., & Alshboul, K. (2023). Islamic financial technology acceptance: An empirical study in Jordan. *International Journal of Data and Network Science*, 7(4), 1659–1668.
8. Alsmadi, I. (2015). Building an Islamic financial information system based on policies and risk management. *Journal of King Saud University – Computer and Information Sciences*, 27(4), 493–500. <https://doi.org/10.1016/j.jksuci.2014.11.001>
9. Alsmadi, M. K. (2025). Beyond compliance: Islamic FinTech and CSR in fostering inclusive financial adoption. *Future Business Journal*, 11(1), 7. <https://doi.org/10.1186/s43093-025-00430-z>
10. Ashraf, S., Robson, J., & Sekhon, Y. K. (2015). Consumer trust and confidence in the compliance of Islamic banks. *Journal of Financial Services Marketing*, 20(2), 133–144. <https://doi.org/10.1057/fsm.2015.8>
11. Ashurov, S., Othman, A. H. A., Kassim, S., & Sharofiddin, A. (2019). The effects of trust mediator and education level moderator on adoption of Islamic banking system in Tajikistan. *Journal of Russian University of Economics*, 5(4), 466–489. <https://doi.org/10.32609/j.ruje.5.33497>
12. Aysan, A. F., Ciftler, B. S., & Unal, I. M. (2024). Predictive power of random forests in analyzing risk management in Islamic banking. *Journal of Risk and Financial Management*, 17(3), 104. <https://doi.org/10.3390/jrfm17030104>
13. D
14. 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>
15. Dawood, H., Hasan, A., & Butt, M. I. (2022). Business trends and challenges in Islamic FinTech: A systematic literature review. *F1000Research*, 11, 109400. <https://doi.org/10.12688/f1000research.109400.1>
16. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
17. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.1060.0080>
18. G
19. Grégoire, Y., Tripp, T. M., & Legoux, R. (2009). When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance. *Journal of Marketing*, 73(6), 18–32. <https://doi.org/10.1509/jmkg.73.6.18>

20. H

21. Haider, M. J., Changchun, G., Akram, T., & Hussain, S. T. (2018). Does gender differences play any role in intention to adopt Islamic mobile banking? *Journal of Islamic Marketing*, 9(3), 439–460. <https://doi.org/10.1108/JIMA-11-2016-0082>
22. Hamsin, M. K., Ibrahim, M. A., & Wan Hussain, W. M. H. (2023). Sharia e-wallet: The issue of Sharia compliance and data protection. *Al-Manahij: Jurnal Kajian Hukum Islam*, 17(1), 85–100. <https://doi.org/10.24090/mnh.v17i1.7633>
23. Hong, Q. N., Fàbregues, S., Bartlett, G., Boardman, F., Cargo, M., Dagenais, P., Gagnon, M.-P., Griffiths, F., Nicolau, B., O'Cathain, A., Rousseau, M.-C., Vedel, I., & Pluye, P. (2018). The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers. *Education for Information*, 34(4), 285–291. <https://doi.org/10.3233/EFI-180221>
24. ICD-LSEG. (2023). Islamic Finance Development Report 2023: Navigating uncertainty. Islamic Corporation for the Development of the Private Sector & London Stock Exchange Group.

25. I

26. Idrees, M. A., Hossain, M. S., & Hossain, M. A. (2024). Comparative analysis of FinTech adoption among Islamic and conventional banking customers. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(1), 100343. <https://doi.org/10.1016/j.joitmc.2024.100343>
27. Irimia-Diéguez, A., Albort-Morant, G., Oliver-Alfonso, M. D., & Ullah, S. (2024). Predicting the intention to use Paytech services by Islamic banking users. *International Journal of Islamic and Middle Eastern Finance and Management*, 17(1), 1–15. <https://doi.org/10.1108/IMEFM-07-2022-0298>
28. Islamic Financial Services Board. (2024). Islamic Financial Services Industry Stability Report 2024. IFSB.

29. J

30. Jamshidi, D. (2016). Forecasting patronage factors of Islamic credit card as a new e-banking service. *Journal of Islamic Marketing*, 7(3), 363–384. <https://doi.org/10.1108/JIMA-07-2014-0050>
31. Jamshidi, D., & Hussin, N. (2016). Islamic banking services adoption as a new banking restructure: Determining the factors. *Humanomics*, 32(2), 151–168. <https://doi.org/10.1108/H-07-2013-0042>

32. K

33. Khan, H. U., & Alibrahim, A. (2023). Utilizing biometric system for enhancing cyber security in banking. *IEEE Access*, 11, 82751–82765. <https://doi.org/10.1109/ACCESS.2023.3298824>
34. Koştı, R., & Kayadibi, S. (2025). Bibliometric analysis of artificial intelligence and machine learning applications for human resource management. *Future Business Journal*, 11(1), 179. <https://doi.org/10.1186/s43093-025-00602-x>

35. L

36. Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, 33(1), 159–174. <https://doi.org/10.2307/2529310>

37. M

38. Mansour, I. H. F., Eljelly, A. M. A., & Abdullah, A. M. (2016). Consumers' attitude towards e-banking services in Islamic banks. *Review of International Business and Strategy*, 26(2), 244–260. <https://doi.org/10.1108/RIBS-02-2014-0024>
39. Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. <https://doi.org/10.2307/258792>
40. Mazumder, M. N. H. (2022). The spillover effect of the Bangladesh Bank cyber heist on banks' cyber risk disclosures in Bangladesh. *Journal of Operational Risk*, 17(2), 1–28. <https://doi.org/10.21314/JOP.2020.249>
41. Mbaidin, H. O., Almomani, Q. A., & Al-Husban, A. A. (2024). The critical success factors of blockchain technology effectiveness on Jordanian Islamic banks' performance. *International Journal of Data and Network Science*, 8(1), 269–278. <https://doi.org/10.5267/j.ijdns.2023.9.024>
42. Mohd Thas Thaker, M. A. B., Mohd Thas Thaker, H., Khaliq, A., Allah Pitchay, A., & Mohd Mydin Meera, A. K. (2019). What keeps Islamic mobile banking customers loyal? *Journal of Islamic Marketing*, 11(6), 1499–1521. <https://doi.org/10.1108/JIMA-08-2017-0090>
43. Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3), 20–38. <https://doi.org/10.2307/1252308>
44. Mulia, D., Usman, H., & Chairy, C. (2021). The role of customer intimacy in increasing Islamic bank customer loyalty in using mobile banking. *Journal of Islamic Marketing*, 12(10), 1948–1966. <https://doi.org/10.1108/JIMA-09-2019-0190>
45. N
46. Naeem, M. (2019). Understanding the role of social networking platforms in addressing the challenges of Islamic banking. *Journal of Management Development*, 38(8), 667–682. <https://doi.org/10.1108/JMD-04-2019-0107>
47. Naeem, M. (2021). Developing the antecedents of social influence for internet banking adoption through social networking platforms. *Asia Pacific Journal of Marketing and Logistics*, 33(8), 1775–1794. <https://doi.org/10.1108/APJML-07-2019-0467>
48. P
49. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Gluud, C., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
50. Parayil Iqbal, K. M. (2023). Integrating trust with extended UTAUT model: A study on Islamic mobile banking adoption in the Maldives. *Journal of Islamic Marketing*, 14(3), 804–826. <https://doi.org/10.1108/JIMA-01-2022-0030>
51. Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know? *Industrial Marketing Management*, 90, 517–524. <https://doi.org/10.1016/j.indmarman.2020.09.005>

52. Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies*, 45(4), 01–016. <https://doi.org/10.1111/ijcs.12695>
53. Pew Research Center. (2025). The world's religious groups: How their sizes changed from 2010 to 2020. Pew Research Center.
54. R
55. R.V., S. H., Annamalai, B., & Chandrasekaran, S. (2024). Consumer behavior in Islamic banking: A systematic literature review and agenda for future research. *Journal of Islamic Marketing*, 15(5), 1326–1349. <https://doi.org/10.1108/JIMA-06-2023-0195>
56. Ridzuan, A. R. (2024). Artificial intelligence in the financial sector: The line between innovation, regulation, and ethical responsibility. *Information*, 15(8), 432. <https://doi.org/10.3390/info15080432>
57. Riza, A. F., Fanani, Z., & Shofawati, A. (2024). Strengthening a sustainable Islamic financial industry through digital banking. *Journal of Islamic Marketing*, 15(8), 2182–2203. <https://doi.org/10.1108/JIMA-01-2023-0025>
58. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
59. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153–176). Guilford Press.
60. S
61. Shahimi, S., Ismail, N., Saad, N. M., Yusuf, M. E., & Ghazali, M. F. (2025). A comprehensive bibliometric analysis of FinTech research from 1968 to 2025. *Future Business Journal*, 11(1), 233. <https://doi.org/10.1186/s43093-025-00652-1>
62. Shinkafi, A. A. (2017). Contemporary Islamic economic studies on Maqasid Shari'ah: A systematic literature review. *Humanomics*, 33(3), 315–334. <https://doi.org/10.1108/H-03-2017-0041>
63. Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*, 9(1), 26–46. <https://doi.org/10.4018/IJISP.2015010102>
64. Stewart, K. J. (2003). Trust transfer on the World Wide Web. *Organization Science*, 14(1), 5–17. <https://doi.org/10.1287/orsc.14.1.5.12810>
65. Sudarsono, H., Nugrohowati, R. N. I., & Tumewang, Y. K. (2020). The effect of COVID-19 pandemic on the adoption of internet banking in Indonesia: Islamic bank and conventional bank. *Journal of Asian Finance, Economics and Business*, 7(11), 789–800. <https://doi.org/10.13106/jafeb.2020.vol7.no11.789>
66. Suhartanto, D., Hapsari, R., Alsyuf, I., Anggraeni, D. M., & Muflih, M. (2022). Millennial loyalty towards artificial intelligence-enabled mobile banking services: Integration of trust and service quality. *Journal of Islamic Marketing*, 13(9), 1998–2014. <https://doi.org/10.1108/JIMA-12-2020-0380>

67. Sumaedi, S., Bakti, I. G. M. Y., Rakhmawati, T., Astrini, N. J., Widiarti, T., & Yarmen, M. (2015). The empirical study of Islamic bank customers' trust: The roles of institutional factors and individual trust. *Journal of Islamic Marketing*, 6(2), 191–209. <https://doi.org/10.1108/JIMA-06-2013-0045>
68. U
69. Unal, I. M. (2022). FinTech, digitalisation, and blockchain in Islamic finance: Retrospective investigation. *Fintech*, 1(4), 388–400. <https://doi.org/10.3390/fintech1040029>
70. V
71. Van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, 84(2), 523–538. <https://doi.org/10.1007/s11192-009-0146-3>
72. Van Eck, N. J., & Waltman, L. (2014). Visualizing bibliometric networks. In Y. Ding, R. Rousseau, & D. Wolfram (Eds.), *Measuring Scholarly Impact: Methods and Practice* (pp. 285–320). Springer. https://doi.org/10.1007/978-3-319-10377-8_13
73. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <https://doi.org/10.2307/30036540>
74. Y
75. Yaseen, S. G., Obeidat, A., & Dingus, R. (2022). Islamic mobile banking smart services adoption and use in Jordan. *International Journal of Islamic and Middle Eastern Finance and Management*, 15(5), 873–892. <https://doi.org/10.1108/IJIF-04-2021-0065>

Figures

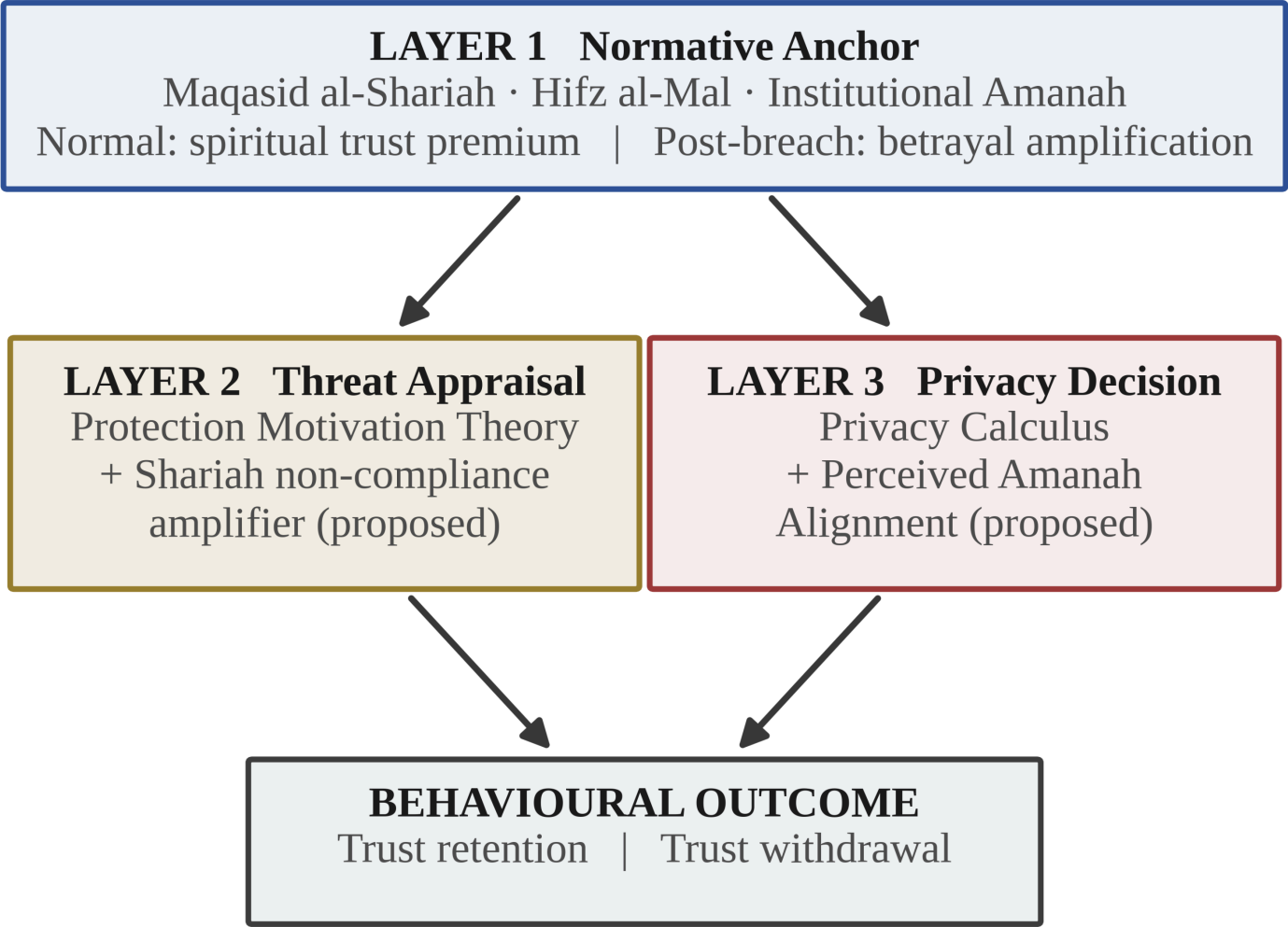


Figure 1

Proposed three-layer conceptual framework for consumer trust, data privacy, and emerging cybersecurity in Islamic digital banking.

Note. Layer 1 feeds simultaneously into Layers 2 and 3; the Shariah non-compliance risk amplifier and Perceived Amanah Alignment are conceptual extensions derived from identified gaps, not empirical findings of the review. Hifz-Al-Aql is deliberately excluded as theologically contestable for information security.

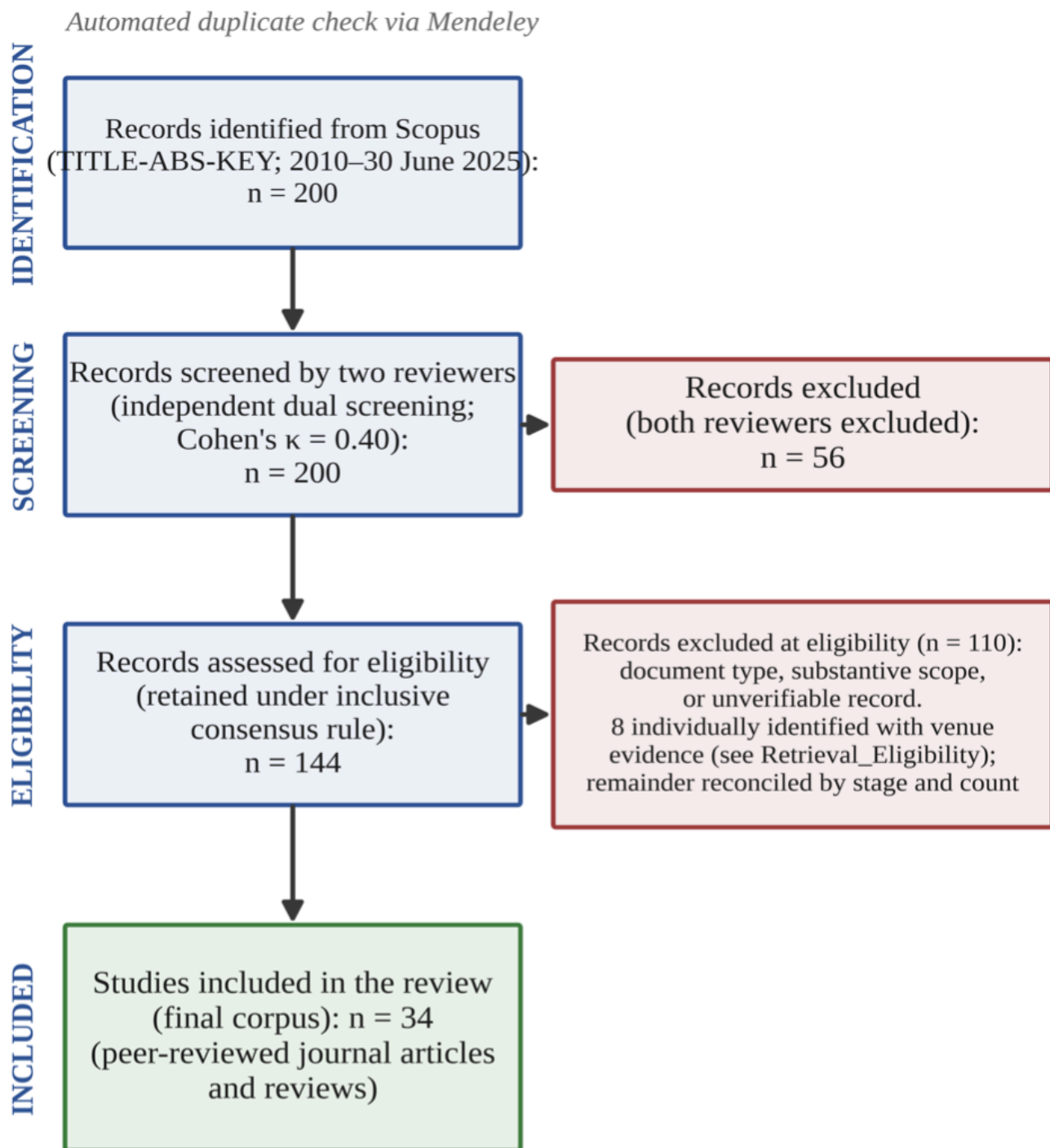


Figure 2

PRISMA 2020 flow diagram

Note. Records flagged as non-English at the screening stage are reported as excluded under the language criterion. The closed data horizon is 30 June 2025 (Page et al., 2021).

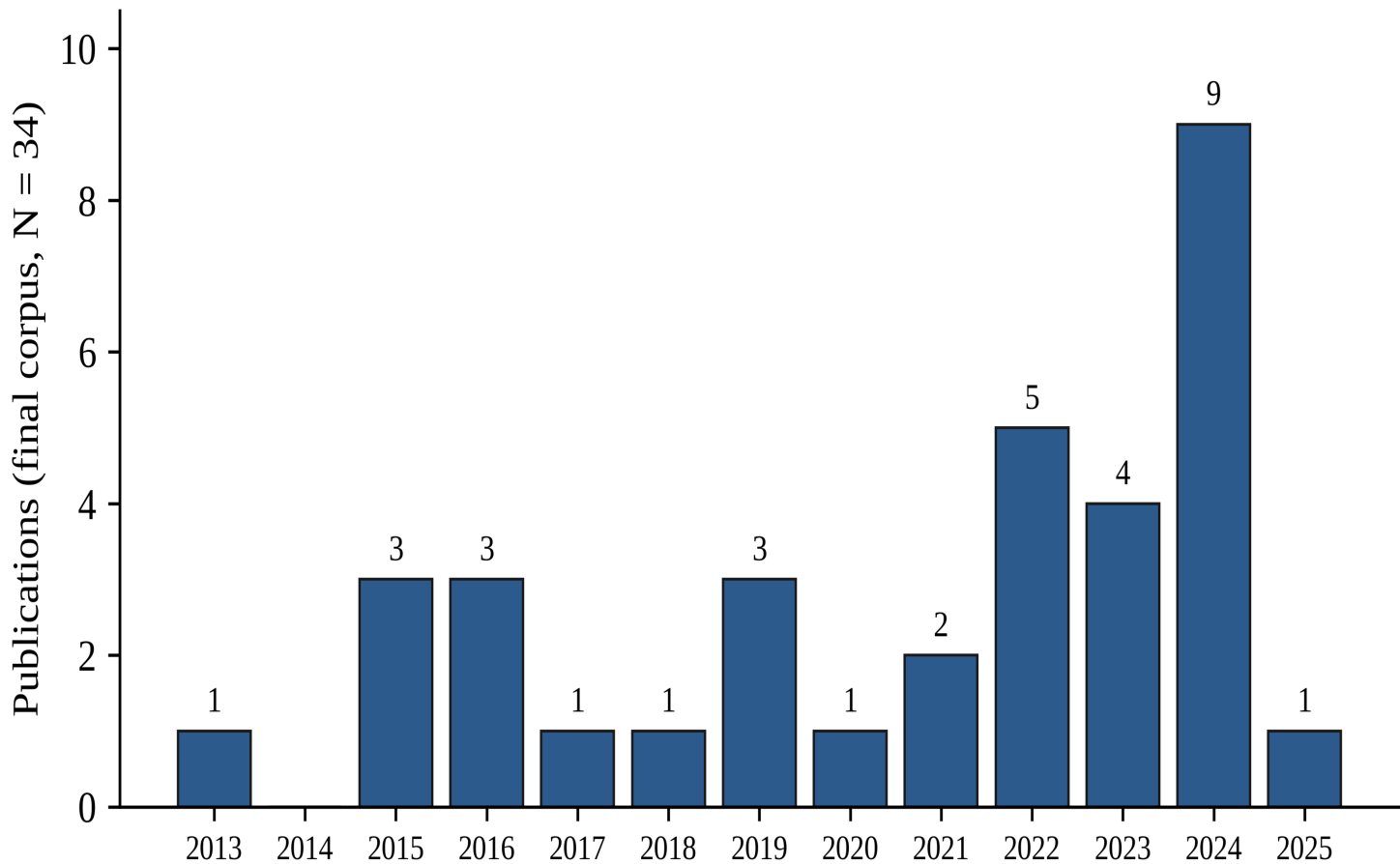


Figure 3

Annual publication trajectory of the final corpus (2013–30 June 2025)

Note. About three-fifths of the corpus (21 of 34) appeared in 2021–2025. Coincidence annotations (no causation implied): the 2020 rise coincides with the COVID-19 shift to contactless and mobile banking; the 2022–2025 acceleration coincides with rising regulatory attention to cyber risk and the proliferation of native Islamic FinTech platforms.

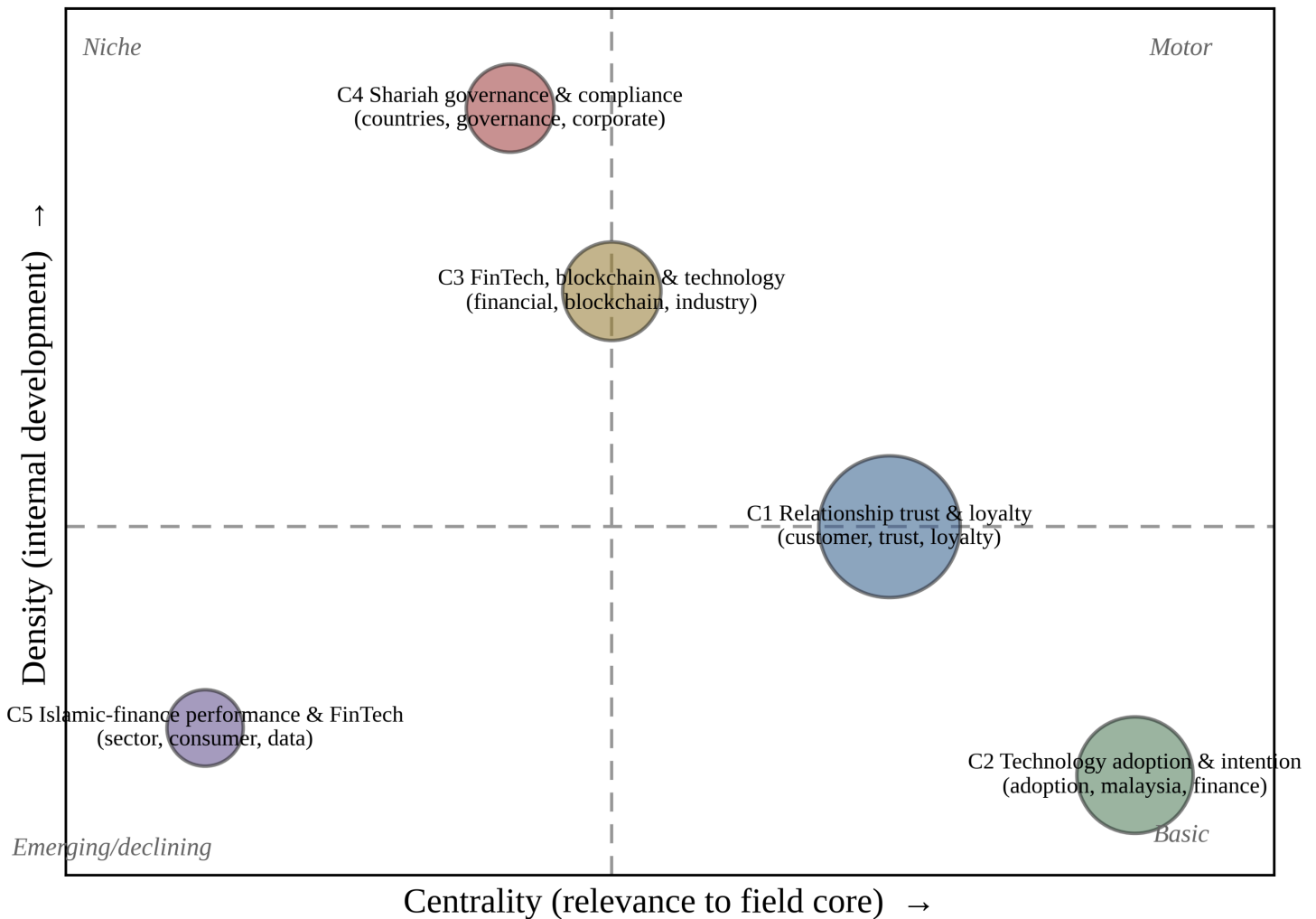


Figure 4

Strategic (thematic) diagram of the title-term clusters (co-word network; minimum occurrence = 5; association-strength normalisation; bubble area proportional to cluster term count)

Note. Cluster positions are computed Callon centrality and density values from the title-term co-word network (Section 3.10); axes are median-split into motor, basic, niche, and emerging quadrants; bubble area is proportional to the number of constituent title terms. The computed centrality and density values for each cluster are reported in the supplementary Master corpus file (Coword_Clusters sheet); the median lines are retained as a visual reference rather than a substantive threshold, and any cluster lying close to a median is interpreted with corresponding caution.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [FBJAppendixA.docx](#)
- [FBJAppendixB.docx](#)

- [FBJAppendixC.docx](#)
- [FBJMasterCorpusDataset.xlsx](#)
- [FBJScreeningandCohenKappaReport.docx](#)