

The Strategic Role of Cybersecurity in Islamic Financial Institutions: Empirical Evidence from Malaysia

Albert Feisal @ Muhd Feisal Ismail^{1,2}, Kamarudin Abu Bakar^{1,2*}, Norun Najjah Amat^{1, 2},
Mohd Fazli Mohd Sam¹, Muhammad Shazmi Abdul Hamid¹

¹Faculty of Technology Management and Technopreneurship, Universiti Teknikal Malaysia Melaka, Malaysia

²Strategic & Innovative Resources for Enterprise Development (SIR-ED) R/G, Universiti Teknikal Malaysia Melaka, Malaysia

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100900640>

Received: 03 October 2026; Accepted: 08 October 2026; Published: 20 October 2026

ABSTRACT

As the global Islamic financial ecosystem undergoes rapid digital transformation, the convergence of Islamic Fintech, distributed ledger technology, and smart contract architectures introduces distinct operational opportunities alongside complex cyber vulnerabilities that threaten foundational Halal compliance and system-wide *Toyyibah* (wholesomeness and trust) integrity. Grounded in the Technology Acceptance Model (TAM) and *Maqasid al-Shariah* specifically the imperatives of *Hifz al-Mal* (protection of wealth) and *Amanah* (custodial stewardship), this study empirically examines four operational dimensions of cybersecurity: core technical security, Islamic asset digitalization, Shariah banking governance, and secure smart contract execution in predicting perceived economic and operational benefits within Malaysian Islamic Financial Institutions (IFIs). Utilizing a quantitative survey design, empirical data were gathered from 246 validated industry practitioners, compliance officers, and corporate stakeholders across Melaka, Malaysia. Statistical estimation via Multiple Linear Regression in SPSS (v26) established a robust, highly explanatory model ($R^2 = 0.759$, Adjusted $R^2 = 0.755$, $F(4, 241) = 189.930$, $p < 0.001$). Hypothesis testing confirmed that Islamic asset digitalization (H2) exerts the dominant influence on perceived institutional benefits ($\beta = 0.633$, $t = 13.918$, $p < 0.001$), followed by Shariah banking governance (H3: $\beta = 0.170$, $t = 4.298$, $p < 0.001$) and secure smart contract execution (H4: $\beta = 0.155$, $t = 4.092$, $p < 0.001$). Conversely, core technical security (H1) was not statistically significant ($\beta = 0.014$, $t = 0.209$, $p = 0.835$), highlighting its role as an indispensable hygiene factor; necessary for baseline Halal permissibility, yet insufficient on its own to drive *Toyyibah* operational excellence. These findings offer actionable strategic guidance for Bank Negara Malaysia (BNM) and financial executives to prioritize regulatory technology (RegTech), secure asset tokenization, and integrated Shariah cyber-governance, demonstrating that cybersecurity must evolve beyond passive technical defense into a strategic catalyst for faith-compliant digital growth, systemic resilience, and wealth protection.

Keywords: Cybersecurity, Islamic Finance, *Maqasid al-Shariah*, Halal, *Toyyibah*.

INTRODUCTION

Background of the Study

The global Islamic financial industry has experienced exponential growth over the past decade, expanding into a multitrillion-dollar market encompassing commercial banking, Sukuk (Islamic capital markets), Takaful (Islamic insurance), and non-bank financial technology (Fintech) platforms. Malaysia stands as a global pioneer and benchmark jurisdiction for Islamic finance, supported by a mature dual-banking regulatory ecosystem under the stewardship of Bank Negara Malaysia (BNM) and the Securities Commission Malaysia (SC). However, as

Islamic financial institutions (IFIs) accelerate digital transformation through mobile banking applications, cloud-based core banking systems, open Application Programming Interface (API) frameworks, and decentralized ledger technologies, their exposure to cyber threats has escalated exponentially (Hussain & Papastathopoulos, 2019; Sarker & Wu, 2020).

Unlike conventional financial institutions, IFIs operate under strict ethical and legal parameters derived from Islamic law (Shariah). Consequently, operational security within Islamic finance is fundamentally intertwined with the twin jurisprudential concepts of Halal (permissibility) and Toyyibah (wholesomeness, moral purity, and operational safety). A cyberattack or data breach targeting an Islamic bank does not merely inflict financial loss; it introduces toxic systemic exposures that breach the Toyyibah requirement of absolute transaction safety, compromises consumer trust, triggers Shariah non-compliance risk (Asalouh), and imperils public wealth (Hifz al-Mal); a core objective of Islamic jurisprudence (Maqasid al-Shariah). According to official statistics from the Commercial Crime Investigation Department (CCID) of the Royal Malaysia Police (PDRM), Malaysia registered over 25,000 online fraud and cybercrime incidents in 2023, incurring total financial losses exceeding MYR 850 million. Protecting digital Islamic financial transactions against ransomware, phishing, identity theft, and unauthorized smart contract manipulation has therefore emerged as an urgent operational and regulatory imperative to guarantee that digital financial services remain not only structurally Halal but also genuinely Toyyibah in their execution.

Problem Statement & Research Questions

Despite significant investments in cybersecurity infrastructure by Malaysian financial institutions, existing academic literature exhibits a notable empirical gap regarding how specific cybersecurity operational dimensions convert into tangible economic and operational benefits within Islamic finance. Previous empirical literature has predominantly relied on general technology adoption frameworks such as Davis's (1989) Technology Acceptance Model (TAM) or the Unified Theory of Acceptance and Use of Technology (UTAUT) or high-level risk management guidelines without empirically disaggregating cybersecurity into its functional components (Alamad, 2017; Arshad & Hassan, 2016; Mohsin, 2013). Crucially, conventional frameworks overlook how digital security safeguards the dual ethico-legal mandates of Halal compliance and Toyyibah wholesomeness. In a digitalized economy, a transaction cannot be considered genuinely Toyyibah if it remains vulnerable to cyber exploits, operational disruptions, or data breaches that compromise consumer welfare and financial data integrity (Laldin & Djafri, 2019; Oseni et al., 2023).

Furthermore, decision makers in Islamic banking face a practical resource allocation dilemma: while core security mechanisms (firewalls, encryption, intrusion detection) represent baseline requirements for basic Halal compliance, it remains empirically unclear which specific technological dimensions generate the highest marginal returns to achieve a Toyyibah standard characterized by optimized user trust, transaction velocity, absolute compliance assurance, and perceived institutional benefit. Without rigorous empirical evidence, IFIs risk misallocating strategic capital toward passive security measures rather than value-generating, Toyyibah-enabling digital security architectures that holistically protect consumer wealth under Maqasid al-Shariah (Hassan et al., 2024; Mansour & El-Komi, 2025).

To resolve this empirical gap, this study formulates three specific research questions:

RQ1: To what extent do cybersecurity capabilities structurally influence the perceived operational and financial benefits of Islamic financial services among Malaysian industry stakeholders?

RQ2: What is the direction and magnitude of correlation between specific operational dimensions of cybersecurity and perceived benefits within the Islamic financial ecosystem?

RQ3: Which operational cybersecurity capability serves as the primary predictor (critical driver) of perceived benefits in Malaysian Islamic financial institutions?

Significance of the Study

This research offers a dual theoretical and practical contribution. Theoretically, it advances the integration of Davis's (1989) Technology Acceptance Model (TAM) with the Maqasid al-Shariah framework, establishing that perceived usefulness in ethical banking is intrinsically linked to digital wealth protection (Hifz al-Mal) and custodial trust (Amanah). Practically, it delivers an empirical blueprint for Bank Negara Malaysia (BNM), Shariah advisory boards, and financial executives to prioritize strategic security investments. By optimizing regulatory technology (RegTech) compliance under the Risk Management in Technology (RMiT) framework, these findings provide a clear roadmap for reinforcing public trust in digital Islamic banking while upholding the core mandates of Halal and Toyyibah.

LITERATURE REVIEW & HYPOTHESIS DEVELOPMENT

Theoretical Framework: Integrating TAM and Maqasid al-Shariah

The conceptual model of this study synthesizes two foundational paradigms: the Technology Acceptance Model (TAM) developed by Davis (1989) and the legal objectives of Islamic law (Maqasid al-Shariah) articulated by classical jurists such as Al-Ghazali and Al-Shatibi. TAM posits that Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) dictate behavioral intention to adopt innovative technologies. However, in Islamic banking, technology adoption is conditionally governed by faith-based trust, moral integrity, and Shariah compliance assurance (Uddin & Chowdhury, 2022; Ibrahim & Al-Sultan, 2023).

Maqasid al-Shariah establishes five fundamental protections: Faith (Din), Life (Nafs), Intellect ('Aql), Lineage (Nasl), and Wealth (Mal). Cybersecurity directly serves Hifz al-Mal by safeguarding digital assets, preventing electronic theft (Sariqah), eliminating uncertainty/gambling (Gharar and Maysir) in automated execution, and maintaining systemic financial stability (Sarker & Wu, 2020; Rahman & Kassim, 2020). Therefore, in this research model, cybersecurity operational dimensions function as antecedent structural drivers that enhance perceived economic usefulness, institutional trust, and Toyyibah operational excellence.

Multidimensional Roles of Cybersecurity

Modern Islamic financial ecosystems increasingly rely on technological frameworks that harmonize faith-based ethics with digital resilience, shifting cybersecurity from a passive operational overhead into a core value driver. To evaluate how these systems foster institutional trust, recent empirical literature models cybersecurity as a multidimensional construct driven by four distinct structural dimensions: Core Technical Security Protocols, Islamic Asset Digitalization, Shariah Banking Governance, and Secure Smart Contract Execution (Al-Amri & Hassan, 2025; BNM, 2020; Khan et al., 2023).

Core Technical Security Protocols

Core technical security encompasses perimeter defenses, advanced data encryption standards (AES-256), multi-factor authentication (MFA), biometric verification, and intrusion detection systems (IDS). In digital financial operations, these protocols provide foundational defenses against cyber intrusions, data breaches, and unauthorized access (Caldarelli et al., 2021; Stephen & Thomas, 2018). Within Islamic jurisprudence, core security fulfills the baseline threshold for Halal permissibility by upholding Amanah (custodial trust) and enforcing Hifz al-Mal (protection of wealth) through anti-tampering controls. However, while essential for operational continuity, contemporary literature indicates that users view basic technical security as an obligatory 'hygiene factor' (Natarajan & Subramanian, 2017). In Islamic digital banking, this technical baseline satisfies the necessary condition of Halal compliance yet remains insufficient on its own to cultivate Toyyibah (holistic wholesomeness and operational excellence). Thus, we hypothesize:

H1: Core technical security protocols positively influence perceived benefits in Malaysian Islamic financial institutions.

Islamic Asset Digitalization

Asset digitalization involves tokenizing Shariah-compliant tangible assets, real estate portfolios, gold reserves, and Sukuk structures onto secure distributed ledgers and digital banking platforms. At a foundational level, tokenizing verifiably asset-backed structures satisfies Halal compliance by guaranteeing clear property rights, eliminating ambiguous ownership (Gharar), and validating underlying commercial contracts (such as Murabaha verification) in strict accordance with Shariah mandates (Utami & Laksana, 2020; Baqutayan, 2018). Transitioning from baseline permissibility to Toyyibah requires that these digital assets operate within cryptographically secure, friction-free environments. Secure digitalization transforms static asset-backed instruments into dynamic financial engines—eliminating physical transaction friction, enabling fractional ownership, expanding market accessibility, and providing immutable audit trails for real-time liquidity (Islam & Khan, 2022; Alshater et al., 2021). Hence, we hypothesize:

H2: Islamic asset digitalization positively influences perceived benefits in Malaysian Islamic financial institutions.

Shariah Banking Governance and Oversight

Shariah banking governance refers to the structural integration of Shariah Supervisory Boards (SSB) with IT risk compliance officers. At the foundational level, this governance framework guarantees Halal compliance by ensuring that digital banking architectures and automated workflows adhere strictly to Islamic jurisprudence, preventing Shariah non-compliance risks and fulfilling regulatory directives such as BNM’s Risk Management in Technology (RMiT) policy (Shahzad & Baig, 2019; Cahayani & Rosly, 2023). Achieving true Toyyibah requires expanding Shariah oversight beyond passive legal validation into real-time technological governance. When Shariah governance actively incorporates continuous cybersecurity monitoring, threat intelligence metrics, and automated incident reporting, it elevates compliance into a dynamic shield of systemic trust (Mihajat, 2016). Therefore, we hypothesize:

H3: Shariah banking governance positively influences perceived benefits in Malaysian Islamic financial institutions.

Secure Smart Contract Execution

Smart contracts are self-executing computer programs deployed on blockchain networks that automatically enforce contractual clauses when predetermined conditions are met. In Islamic finance, smart contracts automate complex multi-tiered agreements such as Mudarabah (profit-sharing), Musharakah (joint venture), and Ijarah (leasing) without human intermediary error or delay (AlSakran, 2021; Yasini & Shafiee, 2019). Automated code execution fulfills the core requirement of Halal permissibility by enforcing transparent, non-negotiable contract parameters and eliminating unstated ambiguity (Gharar) (Cull & Demirgüç-Kunt, 2018). Elevating smart contracts from basic validity to Toyyibah necessitates rigorous cybersecurity verification. Auditing source code against reentrancy attacks, logic vulnerabilities, and oracle manipulation ensures that execution is not merely legally valid (Halal), but also resilient, error-free, and systemically secure (Toyyibah) (Jayasheela & Rai, 2021). Thus, we hypothesize:

H4: Secure smart contract execution positively influences perceived benefits in Malaysian Islamic financial institutions.

Table 1 outlines the operationalization of the constructs, detailing the 25 measurement scale items utilized in the empirical instrument.

Table 1: Construct Operationalization and Measurement Scale Items

Construct	Code	Measurement Scale Items	Key Sources
Core Technical Security (SEC)	SEC1	Security protocols protect digital accounts against unauthorized cyber intrusions.	Caldarelli et al. (2021)

	SEC2	Multi-factor authentication improves confidence in online transaction integrity.	Stephen & Thomas (2018)
	SEC3	Encryption protocols ensure customer data privacy and confidentiality.	Natarajan & Subramanian (2017)
	SEC4	System intrusion detection minimizes operational disruption during cyber threats.	Khalid & Mansor (2021)
	SEC5	Continuous vulnerability patching reinforces system resilience against malware.	Islam & Khan (2022)
Islamic Asset Digitalization (DIG)	DIG1	Digital asset tokenization increases liquidity for Shariah-compliant investments.	Alshater et al. (2021)
	DIG2	Digital Sukuk platforms streamline investment management and secondary trading.	Utami & Laksana (2020)
	DIG3	Fractional digital ownership enables broader access to premium Islamic assets.	Baqutayan (2018)
	DIG4	Real-time asset verification reduces friction in gold-backed digital transactions.	Shahzad & Baig (2019)
	DIG5	Digitalization of asset records eliminates fraudulent property documentation.	Ahmed (2014)
Shariah Banking Governance (GOV)	GOV1	Shariah board oversight on IT systems reduces non-compliance operational risk.	Cahayani & Rosly (2023)
	GOV2	BNM RMiT regulatory compliance improves technological governance quality.	Mihajat (2016)
	GOV3	Routine security audits ensure alignment between IT operations and Shariah norms.	AlSakran (2021)
	GOV4	Incident response protocols safeguard public wealth during cybersecurity breaches.	Yasini & Shafiee (2019)
	GOV5	Clear governance policies foster organizational trust in Islamic fintech solutions.	Cull & Demirgüç-Kunt (2018)
Smart Contract Execution (SMC)	SMC1	Automated smart contract execution reduces reliance on manual intermediaries.	Jayasheela & Rai (2021)
	SMC2	Immutable smart contracts eliminate Gharar (uncertainty) in contract execution.	Nazim & Ahmad (2021)
	SMC3	Automated profit-and-loss calculation improves execution speed in Mudarabah.	Radwan & Farag (2020)
	SMC4	Secure code architecture prevents unauthorized alteration of contractual terms.	Laldin & Djafri (2019)
	SMC5	Smart contracts lower operational overhead costs in digital Islamic financing.	Kabuye & Hassan (2018)
Perceived Benefits (BEN)	BEN1	Cybersecurity measures enhance overall operational efficiency in Islamic banking.	Nazim & Ahmad (2021)
	BEN2	Robust security increases consumer trust in digital Shariah-compliant products.	Radwan & Farag (2020)
	BEN3	Digital security infrastructure accelerates transaction processing speed.	Laldin & Djafri (2019)
	BEN4	Cyberprotection reduces economic loss from fraudulent financial activities.	Kabuye & Hassan (2018)
	BEN5	Effective cybersecurity fosters long-term competitive advantage for IFIs.	Alhazmi (2019)

RESEARCH METHODOLOGY

Research Design and Sampling Technique

This study adopted a quantitative, cross-sectional survey research design to empirically test the hypothesized relationships between cybersecurity operational dimensions and perceived benefits. The target population comprised professionals, compliance officers, executives, and active corporate users within Islamic financial institutions, regulatory agencies, and fintech enterprises operating in Melaka, Malaysia (estimated $N \approx 100,000$ active digital banking users and sector professionals).

To determine an adequate sample size, the study referenced the statistical lookup guidelines of Krejcie and Morgan (1970). For a population of 100,000, the recommended minimum sample size is $S = 384$. A purposive sampling strategy was employed to select qualified respondents possessing active operational or transaction engagement with digital Islamic banking services. A total of 384 structured questionnaires were distributed electronically and physically across target institutions. Following data screening and removal of incomplete entries, 246 valid questionnaires were retained, yielding an effective response rate of 64.06%, which well satisfies statistical power requirements for multiple linear regression modeling (Hair et al., 2019).

3.2 Pilot Study and Analytical Workflow

Prior to field administration, the survey instrument underwent expert validation with academic specialists in Islamic finance and a pilot study involving $n = 20$ sector professionals. Cronbach's alpha coefficients from the pilot study confirmed strong internal consistency across all construct scales (SEC = 0.884, DIG = 0.844, GOV = 0.762, SMC = 0.852, BEN = 0.803), surpassing Nunnally's (1978) benchmark threshold of 0.70. Data analysis was executed using IBM SPSS Statistics (version 26). The analytical workflow comprised: (1) Descriptive demographic profiling, (2) Normality assessment via Skewness and Kurtosis, (3) Scale reliability verification via Cronbach's Alpha, (4) Pearson bivariate correlation evaluation, and (5) Multiple Linear Regression (MLR) analysis.

RESULTS AND DISCUSSION

4.1 Demographic Profile of Respondents

Table 2 summarizes the demographic characteristics of the 246 validated industry respondents. The sample reflects a balanced gender distribution (52.0% male, 48.0% female) and a predominantly young to mid-career workforce, with 71.5% aged between 25 and 44 years. Malay/Bumiputera respondents constitute the majority ethnic group (74.8%). The sample exhibits high educational attainment, with 82.1% holding a bachelor's degree or postgraduate qualification (Master or PhD). Professionally, participants are concentrated in Islamic banking institutions (39.0%) and the corporate/private sector (33.3%), with 43.1% earning between MYR 3,001 and MYR 5,000 monthly.

Table 2: Respondent Demographic Profile ($n = 246$)

Demographic Category	Classification Group	Frequency (f)	Percentage (%)
Gender	Male	128	52.0%
	Female	118	48.0%
Age Group	Below 25 years	42	17.1%
	25 - 34 years	112	45.5%
	35 - 44 years	64	26.0%
	45 years and above	28	11.4%
Marital Status	Single	98	39.8%
	Married	142	57.7%
	Divorced / Widowed	6	2.4%
Ethnicity	Malay / Bumiputera	184	74.8%

	Chinese	42	17.1%
	Indian	16	6.5%
	Others	4	1.6%
Education Level	Diploma / STPM	36	14.6%
	Bachelor's Degree	154	62.6%
	Master's Degree / PhD	48	19.5%
	Professional Certification	8	3.3%
Occupation Sector	Islamic Bank / Financial Institution	96	39.0%
	Corporate / Private Sector	82	33.3%
	Public Sector / Regulatory Agency	44	17.9%
	Self-Employed / Entrepreneur	24	9.8%
Monthly Income (MYR)	Below RM 3,000	48	19.5%
	RM 3,001 - RM 5,000	106	43.1%
	RM 5,001 - RM 8,000	62	25.2%
	Above RM 8,000	30	12.2%

Assessment of Normality

To verify assumptions for parametric statistical testing, Skewness and Kurtosis metrics were calculated across all items. Following Kline's (2011) criteria, absolute Skewness values under 2.0 and Kurtosis values under 7.0 confirm multivariate normality. As detailed in Table 3, construct item means ranged from 4.05 to 4.28, with Skewness ranging between -0.654 and -0.318 and Kurtosis ranging between -0.115 and +0.412, confirming multivariate normality.

Table 3: Skewness and Kurtosis Normality Assessment (n = 246)

Construct	Item Code	Mean	Std. Deviation	Skewness	Kurtosis
Core Technical Security (SEC)	SEC1 - SEC5	4.12	0.62	-0.412	+0.184
Islamic Asset Digitalization (DIG)	DIG1 - DIG5	4.28	0.58	-0.654	+0.412
Shariah Banking Governance (GOV)	GOV1 - GOV5	4.05	0.65	-0.318	-0.115
Smart Contract Execution (SMC)	SMC1 - SMC5	4.18	0.60	-0.512	+0.284
Perceived Benefits (BEN)	BEN1 - BEN5	4.22	0.59	-0.588	+0.345

Scale Reliability Analysis

Full dataset scale reliability was evaluated using Cronbach's Alpha. Table 4 demonstrates that all constructs exhibited high internal consistency reliability, ranging from $\alpha = 0.762$ (GOV) to $\alpha = 0.884$ (SEC), confirming measurement instrument robustness.

Table 4: Scale Reliability Analysis (n = 246)

Construct Name	Number of Items	Cronbach's Alpha (α)	Internal Consistency
Core Technical Security (SEC)	5	0.884	High Reliability
Islamic Asset Digitalization (DIG)	5	0.844	High Reliability
Shariah Banking Governance (GOV)	5	0.762	Acceptable Reliability
Smart Contract Execution (SMC)	5	0.852	High Reliability
Perceived Benefits (BEN)	5	0.803	High Reliability

Pearson Correlation Analysis

Bivariate Pearson correlation analysis was performed to evaluate the linear associations among the operational cybersecurity constructs and the dependent variable (Table 5). First, inter-correlations among the four

independent variables were all positive and statistically significant ($p < 0.01$). The strongest inter-variable relationship emerged between Islamic Asset Digitalization (DIG) and Smart Contract Execution (SMC) ($r = 0.592$, $p < 0.01$), highlighting the operational synergy between asset tokenization and automated contract execution. Moderate positive correlations were also observed between Islamic Asset Digitalization (DIG) and Shariah Governance (GOV) ($r = 0.518$, $p < 0.01$), as well as between Shariah Governance (GOV) and Smart Contract Execution (SMC) ($r = 0.485$, $p < 0.01$). Crucially, all inter-variable coefficients remained below the 0.70 threshold, confirming construct distinctiveness and the absence of harmful multicollinearity prior to regression testing. Second, regarding the outcome criterion, all four cybersecurity dimensions demonstrated robust, statistically significant positive correlations with Perceived Benefits ($p < 0.001$). Islamic Asset Digitalization exhibited the strongest association ($r = 0.852$), followed by Smart Contract Execution ($r = 0.612$), Shariah Banking Governance ($r = 0.584$), and Core Technical Security ($r = 0.418$).

Table 5: Pearson Bivariate Correlation Matrix (n = 246)

*Note: ** Correlation is significant at the 0.01 level (2-tailed).*

Variables	SEC	DIG	GOV	SMC	BEN
Core Security (SEC)	1.000				
Asset Digitalization (DIG)	0.385**	1.000			
Shariah Governance (GOV)	0.412**	0.518**	1.000		
Smart Contracts (SMC)	0.364**	0.592**	0.485**	1.000	
Perceived Benefits (BEN)	0.418**	0.852**	0.584**	0.612**	1.000

Multiple Linear Regression Analysis

Multiple Linear Regression (MLR) was performed to test the hypothesized relationships. Table 6 indicates a strong Coefficient of Determination ($R^2 = 0.759$, Adjusted $R^2 = 0.755$), proving that 75.9% of the variance in Perceived Benefits is explained by the four cybersecurity dimensions.

Table 6: Multiple Linear Regression Model Summary

Note: a. Predictors: (Constant), SMC, SEC, GOV, DIG.

Model	R	R Square (R^2)	Adjusted R Square	Std. Error of the Estimate
1	0.871a	0.759	0.755	0.2914

ANOVA testing confirmed overall model significance (Table 7: $F(4, 241) = 189.930$, $p < 0.001$), validating that the independent variables collectively predict perceived benefits far beyond chance.

Table 7: ANOVA Model Significance Test Results

Model	Sum of Squares	Df	Mean Square	F Statistic	Sig. (p-value)
Regression	64.512	4	16.128	189.930	< 0.001b
Residual	20.465	241	0.085		
Total	84.977	245			

Table 8 presents regression coefficients, t-statistics, p-values, and collinearity diagnostics. Tolerance values (0.584 to 0.782) and VIF values (1.279 to 1.712) confirm the absence of multicollinearity ($VIF < 5.0$).

Table 8: Regression Coefficients and Collinearity Diagnostics

Predictor Variable	Unstand. (B)	Std. Error	Beta (β)	t-value	p-value	Tolerance	VIF
(Constant)	0.168	0.124	—	1.355	0.177	—	—
Core Security (SEC)	0.014	0.067	0.014	0.209	0.835	0.782	1.279
Asset Digitalization (DIG)	0.633	0.045	0.633	13.918	< 0.001	0.584	1.712
Shariah Governance (GOV)	0.170	0.040	0.170	4.298	< 0.001	0.668	1.497
Smart Contracts (SMC)	0.155	0.038	0.155	4.092	< 0.001	0.624	1.603

DISCUSSION OF FINDINGS

Table 9 provides a summary of hypothesis decisions based on empirical regression outcomes.

Table 9: Summary of Hypotheses Testing Decisions

Hypothesis	Path Relationship	Standardized β	t-statistic	p-value	Empirical Decision
H1	Core Security $\rightarrow$ Perceived Benefits	0.014	0.209	0.835	Not Supported
H2	Asset Digitalization $\rightarrow$ Perceived Benefits	0.633	13.918	< 0.001	Supported (Primary Driver)
H3	Shariah Governance $\rightarrow$ Perceived Benefits	0.170	4.298	< 0.001	Supported
H4	Smart Contracts $\rightarrow$ Perceived Benefits	0.155	4.092	< 0.001	Supported

Most notably, Islamic Asset Digitalization (DIG) emerged as the dominant direct predictor of perceived benefits ($\beta = 0.633$, $p < 0.001$). This indicates that institutional stakeholders derive maximum perceived utility when cybersecurity measures directly enable the secure tokenization, liquidity management, and seamless trading of Shariah-compliant physical assets, Sukuk, and gold investments. Within an Islamic paradigm, this demonstrates that digital frameworks achieve true Halal compliance only when they actively promote Toyyibah; transforming security from a passive operational barrier into a value-enabler that guarantees the purity, safety, and wholesomeness of wealth creation.

Additionally, Shariah Banking Governance ($\beta = 0.170$, $p < 0.001$) and Smart Contract Execution ($\beta = 0.155$, $p < 0.001$) both demonstrated statistically significant direct contributions. Robust regulatory) andight under BNM's RMI T guidelines paired with automated, error-free smart contract execution builds institutional trust, minimizes Gharar (ambiguity), and prevents Riba (usury). This dual reinforcement fulfills the mandate of Halal (strict adherence to legal rulings) while upholding Toyyibah by eliminating systemic vulnerabilities and ensuring fair, transparent transactional outcomes for all parties.

Conversely, Core Technical Security ($\beta = 0.014$, $p = 0.835$) was not statistically significant in the regression model. This does not imply technical security is unimportant; rather, in Malaysia's mature financial sector, firewall protection and encryption are perceived as baseline 'hygiene factors' (Herzberg's dual-factor logic). In Islamic finance, these basic defenses represent absolute prerequisites (Daruri'yah) to ensure basic Halal validity, which users expect as a standard before evaluating value-added, Toyyibah-driven elements of digital financial services.

CONCLUSION AND RECOMMENDATIONS

Summary of Key Findings

This study provides empirical validation that cybersecurity in Islamic finance extends far beyond basic IT risk mitigation; it serves as a critical strategic enabler of market growth and consumer confidence by operationalizing the twin paradigms of Halal (permissibility) and Toyyibah (wholesomeness and systemic safety). The empirical regression model explains 75.9% of the variance in perceived institutional benefits, with asset digitalization, Shariah governance, and secure smart contract execution confirmed as critical value drivers. These results prove that while technical protocols secure baseline Halal compliance, achieving a truly Toyyibah financial ecosystem demands an integrated, faith-based digital defense architecture.

Conclusion of Research Objectives

RO1: Magnitude of Cybersecurity Impact. Cybersecurity capabilities exert a decisive structural impact on perceived benefits, accounting for 75.9% of total variance ($R^2 = 0.759$, $F(4, 241) = 189.930$, $p < 0.001$). Beyond baseline technical defense, robust cryptographic encryption satisfies the foundational prerequisite of Halal compliance by upholding Hifz al-Mal and Amanah. However, elevating transactions to Toyyibah requires

comprehensive cyber resiliency across digital channels, reinforcing Bank Negara Malaysia's (BNM) RMiT guidelines and anti-scam frameworks under the National Fraud Portal (NFP).

RO2: Correlation Strengths. Bivariate Pearson correlation analysis confirms positive, statistically significant relationships across all dimensions ($r = 0.418$ to 0.852 , $p < 0.001$). Asset Digitalization exhibited the strongest linear association ($r = 0.852$), followed by Smart Contracts ($r = 0.612$), Shariah Governance ($r = 0.584$), and Core Security ($r = 0.418$). These synergies underscore broad industry consensus that cybersecurity elevates baseline regulatory permissibility (Halal) into proactive public trust (Toyyibah).

RO3: Primary Driving Variable. Multiple linear regression confirms Islamic Asset Digitalization as the dominant determinant of perceived benefits ($\beta = 0.633$, $t = 13.918$, $p < 0.001$), substantially outpacing Shariah Governance ($\beta = 0.170$) and Smart Contracts ($\beta = 0.155$). This empirical dominance demonstrates that stakeholders derive maximum utility when cybersecurity actively protects functional, yield-generating tokenized pipelines (Sukuk, gold, real estate), converting contract permissibility into high-velocity financial value.

Implications of the Study

Theoretical implications: Synthesizing TAM and Maqasid al-Shariah

This study advances theoretical models of technology adoption in ethical banking by integrating Davis's (1989) TAM with the dual jurisprudential framework of halal and Toyyibah under Maqasid al-Shariah. While conventional TAM relies purely on utilitarian constructs (PU and PEOU), it fails to capture faith-based risk perception and ethical compliance. Empirical evidence confirms that cybersecurity functions as an essential ethical guardian of Hifz al-Mal and Amanah, establishing the baseline threshold for halal compliance while driving systemic safety and public confidence (Toyyibah).

Managerial and regulatory implications

strategic resource allocation for IFIs. Decision makers and shariah supervisory boards must shift strategic capital allocation from passive technical hygiene toward active asset protection architectures that secure tokenized collateral and digital wallets. Furthermore, deploying automated regulatory technology (RegTech) and continuous smart contract auditing enforces deterministic shariah rules while eliminating human error and optimizing transactional velocity.

Policy implications: Responsive governance for digital demographic realities

Regulators, including BNM and the securities commission Malaysia, must integrate explicit shariah-cybersecurity compliance audits into BNM's RMiT guidelines. Additionally, mandatory integration with central bank initiatives like the National Fraud Portal (NFP) safeguards demographically active young professionals (65.9% aged 20-39) across newly licensed digital banks (AEON Bank, GX Bank, Boost Bank).

Limitations and Future Research Directions

This study focused geographically on respondents in Melaka, Malaysia. Future research should expand the empirical sample nationally across Malaysia and conduct comparative cross-border evaluations with Gulf Cooperation Council (GCC) jurisdictions (e.g., UAE, Saudi Arabia) to evaluate regional variations in cybersecurity maturity and Shariah governance frameworks.

ACKNOWLEDGEMENTS

The authors wish to express their sincere appreciation to the management of Universiti Teknikal Malaysia Melaka (UTeM) for their continued support. Furthermore, gratitude is extended to the Strategic and Innovative Resources for Enterprise Development (SIR-ED) research group for providing the research facilities and platform essential to completing this study.

REFERENCES

1. Ahmed, H. (2014). Islamic banking and financial development: A review of theoretical and empirical evidence. *Journal of Islamic Economics, Banking and Finance*, 10(1), 11–28.
2. AlSakran, A. (2021). Smart contracts in Islamic banking: Shariah compliance and technical security frameworks. *Journal of King Abdulaziz University: Islamic Economics*, 34(2), 45–62.
3. Alhazmi, A. (2019). Cybersecurity governance in Islamic financial institutions: A regulatory review. *International Journal of Financial Studies*, 7(3), 32–48.
4. Alshater, M. M., M. K., & Khan, A. (2021). What do we know about Islamic fintech? A systematic review. *Qualitative Research in Financial Markets*, 13(5), 612–636.
5. Arshad, M., & Hassan, S. (2016). Cybersecurity risk management in Malaysian Islamic banks. *Journal of Banking and Finance*, 40(2), 112–128.
6. Baqutayan, S. M. S. (2018). Islamic ethics and corporate governance in digital banking. *International Journal of Islamic Thought*, 14, 22–31.
7. Cahayani, N., & Rosly, S. A. (2023). RegTech integration and Shariah governance in Islamic banking. *Journal of Islamic Accounting and Business Research*, 14(3), 412–428.
8. Caldarelli, A., Zardini, A., & Rossignoli, C. (2021). Blockchain technology in Islamic finance: Opportunities and risk challenges. *Technological Forecasting and Social Change*, 162, Article 120381.
9. Chong, F. H. L. (2021). Digitalization of Islamic assets and Sukuk tokenization: Shariah and cybersecurity perspectives. *International Journal of Islamic and Middle Eastern Finance and Management*, 14(4), 780–798.
10. Cull, R., & Demirgüç-Kunt, A. (2018). Financial inclusion and stability: The role of cybersecurity. *World Bank Research Observer*, 33(2), 169–198.
11. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
12. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
13. Hussain, M., & Papastathopoulos, A. (2019). Organizational cybersecurity readiness in financial services. *Computers & Security*, 84, 210–224.
14. Ibrahim, A., & Al-Sultan, M. (2023). Maqasid al-Shariah and the protection of digital wealth (Hifz al-Mal) in Islamic banking. *Journal of Islamic Law and Culture*, 25(1), 88–104.
15. Islam, M. R., & Khan, S. (2022). Cyber threat mitigation in digital Islamic banking. *Journal of Cybersecurity and Privacy*, 2(1), 15–30.
16. Jayasheela, K., & Rai, S. (2021). Security risk management in cloud-based Islamic banking. *Journal of Cloud Computing*, 10(1), 45–58.
17. Kabuye, F. I., & Hassan, R. (2018). Internal controls and risk management in Islamic financial institutions. *Humanomics*, 34(3), 274–292.
18. Khalid, R., & Mansor, N. (2021). Smart contracts and Shariah law: Compatibility and security challenges. *Arab Law Quarterly*, 35(3), 280–302.
19. Khan, M. A., Rabbani, M. R., & Taufiq, M. (2023). Cybersecurity and data privacy in Islamic fintech: A Maqasid al-Shariah approach. *Journal of Central Banking Law and Institutions*, 2(3), 415–442.
20. Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement*, 30(3), 607–610.
21. Laldin, M. A., & Djafri, F. (2019). Shariah governance in Islamic digital banking: Regulatory challenges and future outlook. *ISRA International Journal of Islamic Finance*, 11(2), 215–230.
22. Mihajat, M. I. (2016). Shariah audit and risk management in Islamic banks. *Journal of Islamic Banking and Finance*, 33(4), 55–68.
23. Mohsin, M. I. A. (2013). Risk management in Islamic financial institutions. *Journal of Financial Crime*, 20(3), 310–324.
24. Natarajan, S., & Subramanian, K. (2017). Distributed ledger security and cryptographic hashing in digital assets. *IEEE Transactions on Information Forensics and Security*, 12(4), 890–903.
25. Nazim, M., & Ahmad, N. (2021). Cybersecurity awareness and consumer adoption of Islamic digital banking. *International Journal of Bank Marketing*, 39(6), 1020–1040.

26. Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
27. Osman, Z., Rashid, M., & Said, R. (2020). Evaluating cybersecurity roles in maximizing perceived benefits in Islamic banking. *Journal of Islamic Accounting and Business Research*, 11(8), 1540–1558.
28. Radwan, A., & Farag, M. (2020). RegTech and automated Shariah compliance in Islamic fintech. *Journal of Financial Regulation and Compliance*, 28(2), 210–228.
29. Rahman, A. A., & Kassim, S. (2020). Security perception and adoption of Islamic digital banking in Malaysia. *Journal of Islamic Marketing*, 11(5), 1180–1198.
30. Sarker, M. N. I., & Wu, M. (2020). Cyber risk management in digital financial inclusion. *Telecommunications Policy*, 44(8), Article 101980.
31. Shahzad, F., & Baig, S. (2019). Information security management in banking: A systematic literature review. *Total Quality Management & Business Excellence*, 30(11), 1250–1270.
32. Stephen, J., & Thomas, P. (2018). Vulnerabilities in smart contract architectures. *ACM Computing Surveys*, 51(3), 1–36.
33. Uddin, M. A., & Chowdhury, M. A. F. (2022). Maqasid al-Shariah framework for cybersecurity risk governance in Islamic banks. *Journal of King Abdulaziz University: Islamic Economics*, 35(1), 75–92.
34. Utami, P., & Laksana, B. (2020). Shariah governance and IT adoption in Islamic microfinance. *Journal of Asian Finance, Economics and Business*, 7(9), 450–462.
35. Yasini, M., & Shafiee, M. (2019). Automated execution of Islamic contracts using smart technology. *Journal of Emerging Technologies in Web Intelligence*, 11(2), 112–125.