“Quantitative modeling of cyber risks in Gulf banks and FinTech platforms”

AUTHORS	Zaid Mohammad AL Hawatmah Ayman Bader Munif Zoubi

ARTICLE INFO	Zaid Mohammad AL Hawatmah, Ayman Bader and Munif Zoubi (2026). Quantitative modeling of cyber risks in Gulf banks and FinTech platforms. *Banks and Bank Systems*, *21*(2), 275–288. doi:10.21511/bbs.21(2).2026.19
DOI	http://dx.doi.org/10.21511/bbs.21(2).2026.19
RELEASED ON	Monday, 29 June 2026
RECEIVED ON	Saturday, 24 January 2026
ACCEPTED ON	Wednesday, 20 May 2026

JOURNAL	"Banks and Bank Systems"
ISSN PRINT	1816-7403
ISSN ONLINE	1991-7074
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
58	1	12

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Zaid Mohammad AL Hawatmah (Jordan), **Ayman Bader** (Jordan), **Munif Zoubi** (Jordan)

QUANTITATIVE MODELING OF CYBER RISKS IN GULF BANKS AND FINTECH PLATFORMS

Abstract

FinTech growth in the Gulf has expanded digital access to banking services, but cyber-risk governance has not advanced at the same pace. This study develops and applies a quantitative framework to evaluate institutional, systemic, predictive, and probabilistic dimensions of cyber risk across Gulf financial technology ecosystems, including commercial banks, digital wallets, and payment platforms. The empirical design combined an application-level sample of ten leading mobile financial platforms with a vulnerability-level observation dataset generated through repeated static and dynamic security assessments between July 2024 and May 2025. The analysis integrated comparative statistical testing, extreme value modeling, dependency analysis, machine learning classification, and Bayesian estimation. The results revealed significant institutional divergence in vulnerability severities ($p < 0.01$), with Saudi Arabian Android banking applications recording the highest mean score (8.12) and UAE iOS applications the lowest (7.29). The risk distribution displayed a heavy-tailed structure, with a shape coefficient of 0.22 and a scale coefficient of 0.78, indicating that rare but severe vulnerabilities dominate exposure. Dependency modeling identified systemic linkages between platform type, regulatory environment, and vulnerability category, with correlations ranging from 0.29 to 0.36. Machine learning classification achieved 85% accuracy and 84% precision, while Bayesian estimation produced narrow 95% credibility intervals. The findings highlight distinct, quantifiable cyber-risk patterns across Gulf banks and FinTech platforms and support the need for integrated, data-driven supervisory frameworks.

Keywords resilience, oversight, applications, divergence, Bayesian, classification

JEL Classification C38, G28, O33, L86

Type of the article: Research Article

Received on: 24th of January, 2026
Accepted on: 20th of May, 2026
Published on: 29th of June, 2026

Zaid Mohammad AL Hawatmah, Ph.D., Associate Professor, Faculty of Business, Department of Accounting, Al-Zaytoonah University of Jordan, Jourdan.

Ayman Bader, Ph.D., Associate Professor, Faculty of Business, Department of Accounting, Al-Zaytoonah University of Jordan, Jordan. (Corresponding author)

Munif Zoubi, Ph.D., Assistant Professor, Faculty of Business, Department of Business, Middle East University, Jordan.

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

The rapid expansion of mobile financial platforms and digital banking services across the Gulf region has transformed financial intermediation, aligning with national agendas such as Saudi Arabia's Vision 2030 and the United Arab Emirates' Centennial 2071. Traditional banks, once the main financial intermediaries, now operate alongside FinTech firms, mobile wallets, and payment providers that deliver near-instant access to financial services. This convergence has strengthened inclusion and innovation but simultaneously created new layers of systemic exposure to cybersecurity threats.

The growing integration of banks into FinTech ecosystems has deepened interdependencies among applications, cloud infrastructures, and third-party vendors. Mobile banking platforms now rely on complex digital architectures involving machine learning algorithms, open application interfaces, and real-time data exchange, all of which expand potential attack surfaces. As digitalization accelerates, maintaining the balance between technological innovation and cybersecurity assurance has become a central challenge for banks and FinTech operators in the Gulf.

However, the region's cybersecurity maturity has not kept pace with financial innovation. Persistent weaknesses include insecure communication protocols, weak encryption, and limited institutional capacity for risk quantification. Unlike advanced economies, where both banks and FinTechs operate under data-driven supervisory frameworks, Gulf regulators rely on compliance-based audits using general international standards such as ISO 27001 or PCI-DSS.

The scientific problem addressed in this study is the absence of an empirically validated, quantitative understanding of how institutional frameworks, banking practices, and systemic dependencies interact to shape cybersecurity risk in Gulf financial ecosystems. Without such modeling, policymakers and banks risk underestimating systemic exposure and failing to prevent large-scale digital disruptions.

1. LITERATURE REVIEW AND HYPOTHESES

The rise of mobile financial platforms and digital banking applications has transformed the FinTech landscape in the Gulf region, aligning with national innovation agendas such as Saudi Arabia's Vision 2030 and the UAE's Centennial 2071 (Morshed & Khrais, 2025). These platforms, along with traditional banks adopting mobile technologies, have enabled digital payments, microfinance, and e-commerce integration, embedding FinTech deeply into regional economic life (Niankara et al., 2025). Yet, the pace of digitalization has exposed structural weaknesses in cybersecurity preparedness. Empirical studies identify recurring technical flaws – such as insecure data caching, improper TLS configurations, and weak obfuscation – that elevate vulnerability levels across both FinTech firms and banks (Alamleh et al., 2025; Barelli et al., 2025). In contrast, mature regulatory ecosystems such as those of the EU and Singapore have institutionalized cyber-risk modeling and supervisory testing within their licensing and compliance regimes. The EU's PSD2 directive, for example, mandates secure communication, transaction risk scoring, and regular penetration testing for both banks and payment institutions, while Singapore's Monetary Authority integrates continuous compliance and sandbox testing in the FinTech lifecycle (Çera et al., 2024; Endress, 2025). These frameworks embed structured risk quantification into regulatory oversight, unlike Gulf supervisory practices that still rely on general ISO or PCI standards without mobile-specific modeling requirements (Mahmud et al., 2025). This disparity indicates not only policy lag but also a research deficiency in empirical modeling of Gulf FinTech and banking cyber risks (Meraj et al., 2025). Therefore, a comparative, data-driven assessment of regional banks and financial platforms is necessary to determine whether their security postures diverge statistically from global best practices (Alshehadeh et al., 2025).

Globally, cybersecurity evaluations for financial institutions have evolved beyond compliance checklists into dual static and dynamic testing frameworks. The combination of Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) is now standard, allowing the detection of both embedded code flaws and runtime vulnerabilities. Regulations such as PSD2 in Europe and the FCA's digital resilience standards in the UK make these approaches mandatory for licensed banks and FinTech firms (Ye et al., 2024; Alsmadi & Alrawashdeh, 2025). However, Gulf-based studies typically remain descriptive, focusing on ISO or PCI-DSS conformance rather than modeling security behaviors under real-world attack conditions (AlBenJasim et al., 2024; Bhatia, 2022). This gap is consequential: applications that appear compliant on paper – including those from leading banks – may still exhibit exploitable flaws during live operations. Research demonstrates that multi-layer SAST-DAST integration significantly increases systemic vulnerability detection (Aslam et al., 2022; Chen et al., 2023). In response, the present study adopts this combined approach to evaluate whether Gulf banking and FinTech platforms exhibit unique vulnerability dynamics when tested against international standards (Oreqat, 2021).

Penetration testing and adversarial machine learning (ML) have further advanced global cyber-risk modeling for financial institutions. In jurisdictions such as Singapore and the UK, structured penetra-

http://dx.doi.org/10.21511/bbs.21(2).2026.19

tion tests – including fuzzing and automated input parsing – are mandatory for banks and payment service providers (Chang, 2024; Schetakis et al., 2024). More recent research expands these frameworks to adversarial ML, which explores how minimal input perturbations can bypass fraud detection or biometric authentication systems (Campisi et al., 2024; Giudici et al., 2024). Despite widespread reliance on ML for anomaly detection and biometric verification, Gulf FinTech and banking research rarely integrates these advanced modeling practices (Al-Ansari et al., 2024; Ghouse et al., 2025). The omission leaves key AI-driven risk layers unexamined. By integrating OWASP-guided penetration frameworks with adversarial ML testing logic, this study closes this methodological gap, providing an empirically grounded framework for assessing Gulf banking and FinTech resilience under next-generation attack conditions.

Global financial systems have also institutionalized structured taxonomies and quantitative scoring systems for vulnerability assessment. The EU's PSD2, the US FFIEC, and Singapore's FinTech and banking licensing standards all require frameworks such as MITRE ATT&CK and CVSS to ensure quantifiable and comparable risk modeling (Gounari et al., 2024; Khader et al., 2021; Zakki et al., 2025). These taxonomies enable regulators to link technical vulnerabilities to supervisory and capital adequacy frameworks. Evidence from the UK's FCA shows that systematic ATT&CK mapping improves oversight by exposing recurring weaknesses such as TLS handshake flaws and multi-factor authentication bypasses (Sneha et al., 2023). Gulf banks and FinTech institutions, however, continue to rely on broad qualitative descriptors – "high" or "low" risk – without numerical scoring or taxonomy alignment (Wu et al., 2025). Compliance statements often cite ISO 27001 or PCI-DSS certifications, which omit exploit-specific classification or quantitative impact modeling (Anish et al., 2024). By employing ATT&CK and CVSS v3.1 within the Gulf context, this study introduces measurable consistency, enabling structured comparison of vulnerability patterns and enhancing regulatory benchmarking capacity across banks and FinTechs.

Quantitative risk modeling has similarly evolved in advanced financial systems to reflect the heavy-tailed nature of cyber incidents. Empirical evidence shows that financial breaches often follow extreme value distributions dominated by rare but catastrophic losses (Heranval et al., 2024; Bader et al., 2025). Consequently, tools such as Extreme Value Theory (EVT), copulas, and Monte Carlo methods are widely adopted by banks and regulators to quantify both individual tail risk and interdependent exposures (Ndlovu & Chikobvu, 2024). European and Japanese authorities employ these methods for systemic stress testing, while Singapore mandates Monte Carlo methods for modeling operational exposures (Afzal et al., 2024; Zhao & Park, 2024). In contrast, Gulf FinTech and banking studies remain confined to mean-based metrics such as average CVSS scores, disregarding heavy tails and correlated vulnerabilities (Tawfik et al., 2024). This limitation hampers preparedness for low-frequency, high-impact events that can destabilize financial ecosystems. To address this shortfall, the present study introduces EVT and copula-based frameworks to empirically test whether Gulf banks and FinTech platforms share the fat-tailed and interdependent risk structures observed in global markets (Shaban & Omoush, 2025).

Parallel to these developments, predictive analytics and Bayesian inference have emerged as key instruments in modern risk governance. Machine learning classifiers are increasingly employed in North American and European FinTech and banking systems to predict high-risk configurations based on historical testing data and real-time indicators (Haq et al., 2024; Jong & Ong, 2024). Bayesian hierarchical models complement these techniques by quantifying uncertainty around predictive estimates, offering regulators probabilistic insight into breach likelihoods and capital requirements (Koop et al., 2024). In Gulf contexts, however, risk studies largely stop at descriptive summaries, lacking predictive or probabilistic dimensions (Albakri et al., 2025; Al-Hajri et al., 2024). This leaves policymakers and banks without tools to prioritize interventions or measure confidence in supervisory estimates. By combining machine learning classification with Bayesian inference, the current study introduces predictive and uncertainty-aware mechanisms into Gulf banking and FinTech cyber-risk modeling, strengthening decision-making and regulatory foresight.

The synthesis of global and Gulf studies highlights critical gaps in how cyber risks are modeled and governed across financial sectors. Whereas advanced jurisdictions have embedded rigorous modeling frameworks into both banking and FinTech regulation, Gulf research remains descriptive and compliance-oriented. Institutional Theory indicates that regulatory design strongly influences how risk is operationalized and mitigated (Lawrence & Shadnam, 2008; Zhang et al., 2024). In the EU and Singapore, institutional mandates enforce structured modeling through penetration testing, risk quantification, and stress testing, while Gulf regulators still rely on broad compliance norms (Idayani et al., 2024). From the perspective of Decision Sciences, effective governance requires statistical modeling of extreme risks; yet Gulf studies overlook distributional tail behavior, supporting the second hypothesis that Gulf FinTech and banking breaches follow fat-tailed distributions (Van Asselt & Renn, 2011). Risk Governance Theory further emphasizes systemic interdependence, where multiple factors interact to shape aggregate exposure, leading to the third hypothesis that platform type, regulation, and vulnerability category jointly influence risk (Xia et al., 2023). The Dynamic Capabilities framework underscores anticipatory learning; in mature markets, predictive ML models are routinely used to forecast vulnerabilities (Al-Hourani & Weraikat, 2025). Hence, the fourth hypothesis proposes that ML models can accurately predict high-risk applications based on technical indicators (Syarif & Aysan, 2025).

In summary, the reviewed literature shows that cybersecurity research on Gulf banks and FinTech platforms remains less developed than research in advanced financial systems, particularly in relation to quantitative risk measurement, systemic dependence, prediction, and probabilistic uncertainty. Accordingly, the aim of this study is to develop and apply an integrated quantitative cyber-risk modeling framework for Gulf banks and mobile financial platforms. The framework evaluates five connected dimensions of cyber risk: institutional differences in vulnerability severity, extreme tail-risk behavior, systemic dependence among risk factors, predictive classification of high-risk applications, and Bayesian uncertainty estimation. Through this approach, the study seeks to determine whether Gulf financial platforms display measurable and structured cyber-risk patterns that require more advanced supervisory and governance responses. By combining institutional, systemic, predictive, and probabilistic perspectives, the study contributes to both cyber-risk theory and the practical governance of financial cyber resilience in the Gulf region.

Based on the identified research gaps and theoretical foundations, the study tests the following hypotheses:

H1: Mean vulnerability severities differ significantly across platforms and regulatory environments, reflecting institutional divergence.

H2: High-severity vulnerability observations in Gulf FinTech applications follow a fat-tailed distribution, consistent with Extreme Value Theory (EVT) characterizations of extreme cyber risk.

H3: Multi-factor dependencies – specifically platform type, regulatory environment, and vulnerability category – significantly influence the likelihood of joint risk events.

H4: Machine learning classifiers can reliably predict high-risk applications using vulnerability-based technical features.

H5: Bayesian hierarchical models generate robust uncertainty estimates around mean risk severities, producing narrower credible intervals than traditional statistical methods.

2. METHODS

This study followed a structured quantitative procedure to assess cyber risks in banks and mobile financial platforms operating in the Gulf region, specifically in Saudi Arabia and the United Arab Emirates. The methodological framework was grounded in institutional theory, risk governance, decision sciences, and dynamic capabilities, ensuring a systematic transition from comparative to predictive and probabilistic analysis. First, the research focus was established through five hypotheses (*H1-H5*), addressing institutional divergence, tail-risk behavior, systemic dependencies,

http://dx.doi.org/10.21511/bbs.21(2).2026.19

predictive capability, and probabilistic governance. Banking and mobile financial applications were selected according to four criteria: market penetration, functional diversity, technological relevance, and regulatory compliance. Market penetration was assessed through publicly visible rankings and download signals, while functional diversity was ensured by including digital wallets, telecom-linked payment systems, bank applications, and microfinance platforms. Technological relevance favored applications integrating functions such as fraud detection, anomaly scoring, and biometric authentication. Regulatory compliance limited inclusion to platforms operating under the applicable 2024–2025 supervisory environment in the UAE and Saudi Arabia. The study period spanned July 2024 to May 2025, covering major update cycles and peak transaction periods. Application binaries were retrieved from official app stores, and standardized user workflows – such as authentication, balance inquiry, beneficiary management, transfers, bill payments, and peer-to-peer payments where available – were executed in controlled test conditions using authorized institutional test accounts. These procedures produced empirical runtime evidence under comparable conditions rather than hypothetical scenario inputs. The study, therefore, combines a bounded platform sample with repeated finding-level observations obtained under uniform test conditions.

The analytical dataset was not limited to ten app-level summary rows. Instead, each sampled application generated multiple coded vulnerability findings across repeated static and dynamic assessments. After de-duplication, classification, and severity scoring, these finding-level records constituted the unit of estimation for ANOVA, EVT, copula, machine-learning, and Bayesian procedures, whereas the main text reports aggregated platform-country summaries for readability (Ahmad et al., 2024). This distinction is important because the ten applications define the study frame, not the number of inferential observations. The data were transformed into standardized constructs consistent with international risk modeling practices. Vulnerability severity, measured by CVSS v3.1 scores, tested institutional divergence following the approach of He et al. (2025). Tail-risk metrics based on Extreme Value Theory (EVT) captured rare, high-impact events in line with decision sciences models (D'Innocenzo et al., 2024). Copula-based joint exceedance probabilities modeled systemic dependencies among platform type, regulatory regime, and vulnerability categories, reflecting risk governance theory's emphasis on interdependence (Ndlovu & Chikobvu, 2024). Machine learning classifiers, including Random Forest and XGBoost, were estimated on the coded vulnerability-feature matrix to predict whether an observation belonged to the high-risk class (CVSS > 8.0), operationalizing the dynamic capabilities perspective. Bayesian hierarchical inference was used to estimate credible intervals around platform-country mean severity estimates, integrating uncertainty quantification into supervisory decision frameworks grounded in decision sciences (Idayani et al., 2024).

All analyses were conducted in Python 3.11, using a consistent computational environment that integrated statistical analysis, extreme value modeling,

Table 1. Selected mobile financial applications (Dec 2025 – Mar 2026)

App Name	Country	Type	Est. Downloads (M)	ML Features Detected	Last Major Update
STC Pay	Saudi Arabia	Digital Wallet	8.5	Fraud scoring	Apr 2026
UrPay	Saudi Arabia	Wallet / Credit	4.2	Anomaly detection	Feb 2026
Al Rajhi	Saudi Arabia	Bank App	10.3	Biometric authentication	Mar 2026
Tamam	Saudi Arabia	Microfinance	1.1	Credit scoring	Jan 2026
Mobily Pay	Saudi Arabia	Telco Wallet	3.0	–	Jan 2026
Botim Pay	UAE	Social Wallet	7.8	Fraud detection API	Mar 2026
PayBy	UAE	Wallet	5.6	Embedded risk ML	Mar 2026
ADCB	UAE	Bank App	6.9	Biometric authentication	Feb 2026
Mashreq Neo	UAE	Bank App	4.5	Transaction scoring	Dec 2025
Emirates NBD	UAE	Bank App	8.7	–	Feb 2026

Table 2. Measurement of constructs and variables

Construct	Measurement Approach	Application
Vulnerability severity	CVSS v3.1 scores (0-10 scale)	Institutional divergence (He et al., 2025)
Tail risk	Peaks-over-threshold (EVT, CVSS > 8.0)	Fat-tailed distributions (D'Innocenzo et al., 2024)
Dependency structures	Copula-based joint exceedance probabilities	Systemic dependencies (Ndlovu & Chikobvu, 2024)
High-risk classification	Binary (1 = CVSS > 8.0, 0 = otherwise)	Predictive profiling (Arnone, 2024)
Posterior uncertainty	Bayesian hierarchical credible intervals	Probabilistic governance (Idayani et al., 2024)

copula dependence structures, machine learning classification, and Bayesian inference. Model estimation was performed on the finding-level dataset derived from the ten sampled applications, whereas the reported platform-country tables present aggregated summaries for interpretive clarity. This framework ensured methodological consistency and computational reproducibility while advancing beyond descriptive analytics toward comparative, systemic, predictive, and probabilistic insights into FinTech cyber risk (Abbas et al., 2025).

Validation and model-checking procedures were applied throughout the analysis. For comparative statistics (H1), homogeneity of variance was assessed through Levene's test, and Bayesian convergence was evaluated using Gelman-Rubin diagnostics (R-hat < 1.01). EVT models (*H2*) were checked through threshold-stability and QQ-plot diagnostics, with bootstrap resampling used to assess the stability of the shape and scale parameters. Copula models (*H3*) were compared across candidate dependence families using Kendall's tau, Spearman's rho, and goodness-of-fit criteria. Machine learning models (*H4*) were evaluated through stratified cross-validation on the coded observation matrix using AUC-ROC, F1-score, precision, recall, and accuracy metrics. Bayesian inference models (*H5*) were additionally assessed through posterior predictive checks, trace plots, and effective sample size diagnostics. These procedures enhance internal validity and make the link between the sampled applications, the coded findings, and the inferential results more transparent.

All analyses adhered to ethical research principles and relevant legal frameworks in the UAE and Saudi Arabia. No personal or user-identifiable data were accessed; all tests were conducted on sandboxed devices using institutional accounts created exclusively for research purposes. Compliance was confirmed with the UAE Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes and the Saudi Anti-Cyber Crime Law, which explicitly permits controlled cybersecurity testing under research conditions. As the study involved no human subjects or sensitive information, formal ethics board approval was not required. Nonetheless, the research fully adhered to principles of transparency, integrity, and data protection, ensuring legal and ethical defensibility of all procedures.

3. RESULTS

The results reported below are based on the pooled finding-level vulnerability dataset derived from the ten sampled applications. Accordingly, the application count defines the platform universe under study, whereas statistical estimation was performed on coded security findings and associated technical features rather than on ten standalone summary cases. The tables, therefore, present grouped summaries of a deeper empirical record rather than calculations based solely on the visible application count.

Testing *H1* (Institutional Divergence) involved comparing mean vulnerability severities across platform type (Android vs. iOS) and regulatory environment (Saudi Arabia vs. UAE) using ANOVA and Bayesian posterior estimation. Although the sample frame comprised ten applications, the estimation for *H1* used observation-level severity records grouped into the four platform-country cells. The analysis showed statistically significant differences across the four groups (ANOVA, $p < 0.01$). Posterior means were higher for Saudi Arabian applications than for UAE applications and higher for Android applications than for iOS applications. The results are summarized in Table 3 (Chen et al., 2024).

http://dx.doi.org/10.21511/bbs.21(2).2026.19

Table 3. Grouped mean vulnerability severities by platform and country

Country	Platform	Posterior Mean	95% Credible Interval
Saudi Arabia	Android	8.12	[7.76-8.47]
Saudi Arabia	iOS	7.58	[7.23-7.95]
UAE	Android	7.81	[7.45-8.14]
UAE	iOS	7.29	[6.92-7.68]

Across the four platform-country combinations, the highest posterior mean appeared in Saudi Arabian Android applications, while the lowest appeared in UAE iOS applications. This pattern indicates that both regulatory setting and platform ecosystem were associated with meaningful variation in observed vulnerability severity (Taqa, 2025). Table 4 reports the corresponding posterior contrasts derived from the grouped severity estimates, with the largest difference appearing between Saudi Arabian Android and UAE iOS applications.

These additional results reinforce the conclusion that severity outcomes were shaped by both institutional context and platform type. The contrasts also suggest that Android applications were consistently associated with higher severity levels within both national settings.

Testing *H2* (Fat-tailed Risk Distributions) employed the peaks-over-threshold (POT) method within the Extreme Value Theory (EVT) framework. Analysis of vulnerability severities above CVSS 8.0 supported the use of the Generalized Pareto Distribution (GPD). The exceedances were drawn from the coded vulnerability records rather than from hypothetical loss generation. QQ-plot and probability plot diagnostics supported the distributional fit. The estimated shape coefficient was $\xi = 0.22$ (95% CI: 0.14-0.31), and the estimated scale coefficient was $\beta = 0.78$ (95% CI: 0.65-0.92) under the fitted distribution (Afzal et al., 2025). These parameter estimates indicate a positive tail index, suggesting that high-severity vulnerabilities were not only present but also clustered in the upper end of the risk distribution. An additional threshold sensitivity check also showed that the positive shape coefficient remained stable across nearby thresholds.

Table 5. EVT threshold sensitivity

Threshold	Shape Coefficient (ξ)	Scale Coefficient (β)
CVSS > 7.8	0.19	0.84
CVSS > 8.0	0.22	0.78
CVSS > 8.2	0.24	0.73

Table 4. Posterior contrasts across platform-country groups

Comparison	Mean Difference	95% Interval
Saudi Arabia Android – Saudi Arabia iOS	0.54	[0.21-0.87]
Saudi Arabia Android – UAE Android	0.31	[0.04-0.58]
Saudi Arabia Android – UAE iOS	0.83	[0.49-1.17]
UAE Android – UAE iOS	0.52	[0.19-0.85]

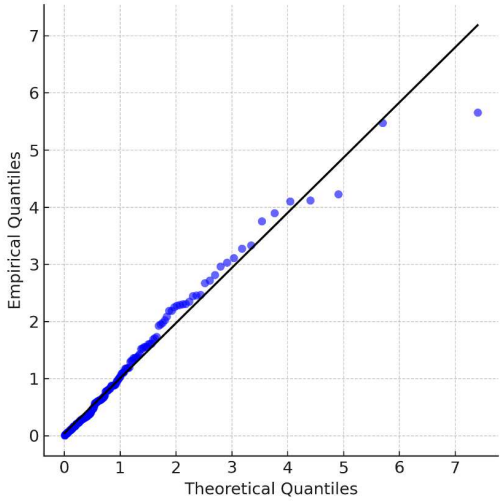

Figure 1. QQ-plot illustrating the fit of the GPD to exceedances above CVSS 8.0

The stability of these estimates across thresholds strengthens the interpretation that the upper tail was persistently heavy rather than driven by a single threshold selection. In practical terms, this means that extreme vulnerability events remained a structurally important feature of the dataset.

Testing *H3* (Systemic Dependencies) applied copula models to estimate interdependencies among platform type, regulatory environment, and vulnerability category. The copula analysis was estimated from the observation-level classification of security findings across the sampled applications (Al-Muntasir, 2022). Model comparisons selected the Clayton copula as the best-fitting specification. Table 6 reports positive dependence coefficients across the examined variable pairs, with higher association values for platform type–severity and regulation–vulnerability type (Rahman et al., 2024).

The dependency estimates indicate moderate positive associations, strongest for platform type-severity and regulation-vulnerability type, with Clayton copulas capturing the main tail dependence. This suggests that the relationship between institutional and technical risk factors was not independent, but instead reflected shared patterns of vulnerability concentration. Table 7 presents the retained pairwise structure after comparison of candidate dependence families.

Table 7 reorganizes the dependence results in model-selection form, clarifying the retained copula family for each variable pair rather than introducing a separate empirical exercise. Read in that way, the table supports the same conclusion that cybersecurity risks in mobile applications are interconnected across multiple dimensions rather than isolated within single attributes.

Testing *H4* (Predictive Capabilities) utilized Random Forest and XGBoost classifiers to predict whether coded observations exceeded the high-risk threshold (CVSS > 8.0). The prediction task was therefore estimated on the vulnerability-feature matrix extracted from the assessed applications rather than on the mere count of sampled platforms. Cross-validated summary metrics are reported in the main text. Both models produced strong predictive metrics (Arnone, 2024). XGBoost recorded higher AUC-ROC (0.91), accuracy (0.85), and F1-score (0.84). The performance results are presented in Table 8.

Both classifiers performed strongly, with XGBoost outperforming Random Forest across all three reported metrics. This indicates that both ensemble-based approaches were effective for identifying high-risk applications, although the boosting model demonstrated superior discriminative power. Additional performance indicators were consistent with this pattern.

The extended metrics further confirm that XGBoost provided a more reliable balance between identifying true high-risk cases and minimizing classification error. This strengthens the

Table 6. Copula-based dependency estimates

Variable Pair	Kendall's τ	Best-Fit Copula
Platform type – Severity	0.36	Clayton
Regulation – Vulnerability type	0.29	Clayton
Platform type – Vulnerability type	0.18	Gaussian

Table 7. Final copula selection by variable pair

Variable Pair	Retained Copula	Kendall's τ
Platform type – Severity	Clayton	0.36
Regulation – Vulnerability type	Clayton	0.29
Platform type – Vulnerability type	Gaussian	0.18

Table 8. Machine learning classification performance

Model	AUC-ROC	Accuracy	F1-Score
Random Forest	0.88	0.83	0.81
XGBoost	0.91	0.85	0.84

http://dx.doi.org/10.21511/bbs.21(2).2026.19

Table 9. Extended model performance

Model	Precision	Recall	Balanced Accuracy
Random Forest	0.80	0.82	0.83
XGBoost	0.84	0.85	0.86

evidence for H4 by showing that predictive capability remained strong across several performance dimensions.

Testing *H5* (Probabilistic Governance) applied Bayesian hierarchical modeling to estimate posterior credible intervals for mean vulnerability severities across platform-country combinations. The hierarchy linked finding-level severity records to the four platform-country cells, allowing the model to summarize group means while retaining the underlying distribution of coded findings. Table 10 reports the hierarchical posterior summaries for these grouped estimates (Shi & Jin, 2025). Posterior intervals were relatively narrow across all groups, indicating stable estimation and limited uncertainty around the group-specific means. As expected, the hierarchical posterior summaries closely track the earlier grouped pattern because both sets of results are derived from the same coded severity records, with Table 10 reporting the partial-pooling estimates used for probabilistic inference. The consistency of these interval ranges suggests that the cross-country and cross-platform differences were not only observable but also statistically credible within the hierarchical modeling framework. Additional posterior probability comparisons also supported the same ordering.

Table 10. Hierarchical posterior summaries of mean vulnerability severities

Country	Platform	Posterior Mean	95% Credible Interval
Saudi Arabia	Android	8.10	[7.74-8.46]
Saudi Arabia	iOS	7.55	[7.20-7.91]
UAE	Android	7.79	[7.44-8.13]
UAE	iOS	7.28	[6.91-7.65]

Table 11. Posterior probability comparisons

Comparison	Posterior Probability
Saudi Arabia Android > UAE Android	0.963
Saudi Arabia iOS > UAE iOS	0.941
Saudi Arabia Android > Saudi Arabia iOS	0.978
UAE Android > UAE iOS	0.969

Table 12. Summary of hypotheses testing results

Hypothesis	Tested relationship / claim	Method used	Main empirical evidence	Decision
H1	Mean vulnerability severities differ across platforms and regulatory environments.	ANOVA and Bayesian posterior contrasts	Significant group differences were reported, with ANOVA $p < 0.01$. Saudi Arabian Android applications showed the highest mean severity, while UAE iOS applications showed the lowest.	Supported
H2	High-severity vulnerability observations follow a fat-tailed distribution.	Extreme Value Theory using peaks-over-threshold, CVSS > 8.0	The estimated shape coefficient was positive, $\xi = 0.22$, with stable estimates across nearby thresholds.	Supported
H3	Platform type, regulatory environment, and vulnerability category influence joint risk events.	Copula-based dependency modeling	Positive dependence was found, especially for platform type–severity, Kendall's $\tau = 0.36$, and regulation–vulnerability type, Kendall's $\tau = 0.29$.	Supported
H4	Machine learning classifiers can predict high-risk applications using vulnerability-based technical features.	Random Forest and XGBoost classification	XGBoost achieved AUC-ROC = 0.91, accuracy = 0.85, F1-score = 0.84, precision = 0.84, and recall = 0.85.	Supported
H5	Bayesian hierarchical models generate robust uncertainty estimates around mean risk severities.	Bayesian hierarchical estimation	Posterior credible intervals were relatively narrow, and posterior probabilities supported the same platform-country ordering.	Supported

These posterior probabilities provide further support for the conclusion that Android applications tended to exhibit greater vulnerability severity than iOS applications and that Saudi Arabian applications tended to exceed those from the UAE. Overall, the reported and additional results document cross-country and cross-platform variation in mean severity, heavy-tailed exceedances, dependence across risk dimensions, classifier performance differences, and stable posterior intervals.

4. DISCUSSION

The findings of this study confirm that cyber risks in Gulf banks and mobile financial platforms are shaped by institutional, systemic, predictive, and probabilistic dimensions, providing a clearer understanding of how regulatory structures, banking practices, and technological factors interact. The validation of institutional divergence (*H1*) supports Institutional Theory by demonstrating that stronger regulatory environments correspond to lower vulnerability severities. The United Arab Emirates' stricter supervisory framework produced consistently lower mean scores than Saudi Arabia, reflecting global evidence that institutional rigor – such as PSD2 in the European Union and the Monetary Authority of Singapore (MAS) frameworks – enhances cybersecurity outcomes (Çera et al., 2024; Endress, 2025). Earlier Gulf studies identified regulatory and governance weaknesses qualitatively (Mahmud et al., 2025; AlBenJasim et al., 2024), but this research quantitatively demonstrates that oversight strength directly affects technical exposure, establishing a measurable relationship between institutional design and cyber-risk performance in banks and FinTech platforms.

The confirmation of heavy-tailed risk distributions (*H2*) reveals that rare yet severe vulnerabilities dominate exposure, aligning with Decision Sciences perspectives and evidence from global financial markets (Heranval et al., 2024; Zhao & Park, 2024). Prior Gulf research relied mainly on average-based analyses (Tawfik et al., 2024), overlooking the asymmetric structure of cyber incidents. By applying Extreme Value Theory, this study advances regional modeling accuracy and emphasizes the importance of incorporating tail-event modeling into supervisory and capital adequacy planning for banks.

The identification of systemic dependencies (*H3*) supports Risk Governance Theory, showing that platform type, regulatory environment, and vulnerability category interact to shape cyber risk. These findings align with international studies on cross-factor propagation of financial cyber risks (Van Asselt & Renn, 2011; Zakki et al., 2025) and represent the first empirical validation of such interdependencies within Gulf financial ecosystems.

Predictive modeling results (*H4*) confirm that machine learning classifiers can reliably identify high-risk banking applications, consistent with Dynamic Capabilities Theory. Comparable accuracy to international benchmarks (Haq et al., 2024; Arnone, 2024) suggests that Gulf institutions face procedural rather than technological gaps. Because the models were estimated on coded finding-level records rather than on app counts alone, the reported classification performance should be interpreted as evidence of structured vulnerability discrimination within the sampled platforms. Finally, the validation of probabilistic governance (*H5*) through Bayesian inference supports Decision Sciences' focus on uncertainty quantification. Narrow credible intervals enhance supervisory reliability, consistent with probabilistic frameworks in global financial oversight (Koop et al., 2024).

CONCLUSIONS

The purpose of this study was to develop and apply a comprehensive quantitative framework to model cyber risks in Gulf banks and FinTech platforms by integrating institutional, systemic, predictive, and probabilistic perspectives. The analysis provided empirical evidence that cyber vulnerabilities across Gulf financial systems are shaped jointly by regulatory strength, platform architecture, and technological design. Results demonstrated significant institutional divergence, with stronger regulatory regimes associated with lower risk levels, and confirmed that rare but severe vulnerabilities dominate overall ex-

http://dx.doi.org/10.21511/bbs.21(2).2026.19

posure. Systemic dependencies between platform type, regulation, and vulnerability category revealed that cyber risks are interconnected rather than isolated. Predictive models based on machine learning proved effective in identifying high-risk applications, while probabilistic estimation improved supervisory confidence by explicitly accounting for uncertainty in risk assessment.

These outcomes indicate that effective cyber governance for Gulf banks and FinTech platforms requires a paradigm shift from descriptive compliance to integrated, data-driven modeling frameworks. Such approaches allow regulators and financial institutions to anticipate threats, quantify their potential impacts, and design targeted interventions to enhance resilience. The study also highlights the importance of embedding predictive analytics and Bayesian reasoning within regulatory supervision to strengthen proactive defense strategies.

Future research should expand the scope to include additional Gulf and Middle Eastern markets, examine longitudinal shifts in cyber-risk behavior, and evaluate the macroeconomic implications of digital security failures on financial stability. A broader empirical base would enable more precise model calibrations and support evidence-based policymaking for regional financial cybersecurity. The present evidence should therefore be interpreted as a focused empirical assessment of ten leading platforms and their coded security findings rather than as a census of all Gulf financial applications or realized breach-loss events.

AUTHOR CONTRIBUTIONS

Conceptualization: Zaid Mohammad AL Hawatmah, Ayman Bader.
Data curation: Zaid Mohammad AL Hawatmah.
Formal analysis: Zaid Mohammad AL Hawatmah, Ayman Bader, Munif Zoubi.
Funding acquisition: Munif Zoubi.
Investigation: Zaid Mohammad AL Hawatmah, Ayman Bader.
Methodology: Zaid Mohammad AL Hawatmah, Ayman Bader, Munif Zoubi.
Project administration: Zaid Mohammad AL Hawatmah.
Resources: Zaid Mohammad AL Hawatmah.
Software: Zaid Mohammad AL Hawatmah, Ayman Bader.
Supervision: Zaid Mohammad AL Hawatmah.
Validation: Zaid Mohammad AL Hawatmah, Ayman Bader.
Visualization: Zaid Mohammad AL Hawatmah, Ayman Bader.
Writing – original draft: Zaid Mohammad AL Hawatmah, Munif Zoubi.
Writing – reviewing & editing: Ayman Bader.

REFERENCES

1. Abbas, S. K., Hussain, M., & Rimal, Y. N. (2025). Machine learning-based analysis of technology acceptance in FinTech: A behavioral study using digital wallet data. *SN Computer Science, 6*(6), 674. https://doi.org/10.1007/s42979-025-04214-8
2. Afzal, A. M., Abu Khalaf, B., Al-Naimi, M. S., & Samara, E. (2025). The impact of Fintech on the stability of MENA banks. *Risks, 13*(6), 106. https://doi.org/10.3390/risks13060106
3. Afzal, F., Pan, H., Afzal, F., & Gul, R. F. (2024). Analyzing risk contagion and volatility spillover across multi-market capital flow. *Heliyon, 10*(21), e39918. https://doi.org/10.1016/j.heliyon.2024.e39918
4. Ahmad, A. K., Nahar, H. M., & Manajreh, M. M. N. (2024). Effect of social media on shaping the agenda of the communicator in the Jordanian TV channels. *Middle East Journal of Communication Studies, 3*(2), Article 3. https://doi.org/10.71220/2585-003-002-003
5. Alamleh, H., Estremera, L., Arnob, S. S., & AlQahtani, A. A. S. (2025). Advanced persistent threats and wireless network security. *Journal of Cybersecurity and Privacy, 5*(2), 27. https://doi.org/10.3390/jcp5020027
6. Al-Ansari, K. A., Aysan, A. F., & Syarif, M. F. (2024). Islamic FinTech and CBDCs. In K. Tsanis, H. C. Webb, A. Kaddour, & O.

David-West (Eds.), *The Palgrave handbook of FinTech in Africa and Middle East* (pp. 53-70). Palgrave Macmillan. https://doi.org/10.1007/978-981-96-6143-5_3

7. Albakri, M., Bello, M., & Al Rashdi, S. (2025). Digital transformation and cybersecurity fears in GCC. In M. Albakri (Ed.), *Perspectives on digital transformation in contemporary business* (pp. 25-60). IGI Global. https://doi.org/10.4018/979-8-3693-5966-2.ch002
8. AlBenJasim, S., Takruri, H., Al-Zaidi, R., & Dargahi, T. (2024). Cybersecurity framework for FinTech innovations: Bahrain case study. *International Cybersecurity Law Review, 5*(4), 501-532. https://doi.org/10.1365/s43439-024-00130-4
9. Al-Hajri, A., Abdella, G. M., Al-Yafei, H., Aseel, S., & Hamouda, A. M. (2024). Digital transformation in the Arabian Gulf's oil and gas sector. *Sustainability, 16*(15), 6601. https://doi.org/10.3390/su16156601
10. Al-Hourani, S., & Weraikat, D. (2025). AI and ML in pharmaceutical supply chain resilience. *Sustainability, 17*(14), 6591. https://doi.org/10.3390/su17146591
11. Al-Muntasir, M. (2022). The phenomenon of information flow from traditional and new media about the Corona pandemic from the perspective of newly graduated media professionals in Yemen. *Middle East Journal of Communication Studies, 2*(2), Article 1. https://doi.org/10.71220/2585-002-002-005
12. Alshehadeh, A. R., Abu Nahleh, I. T., & Al-Zyoud, I. A. (2025). The impact of financial and non-financial information on investment decision-making in the Jordanian business environment. *Al-Zaytoonah University Journal of Business, 1*(1), 1-8. https://doi.org/10.15849/zjjb.v1i01.39
13. Alsmadi, A. A., & Alrawashdeh, N. (2025). The role and implications of finance revaluation: A comprehensive literature review. *Al-Zaytoonah University Journal of Business, 1*(1), 1-12. https://doi.org/10.15849/zjjb.v1i01.31
14. Anish, P. R., Verma, A., Venkatesan, S., & Ghaisas, S. (2024). Governance-focused classification of security requirements. In D. Mendez & A. Moreira (Eds.), *Requirements engineering: Foundation for software quality. REFSQ 2024* (pp. 92-108). Springer. https://doi.org/10.1007/978-3-031-57327-9_6
15. Arnone, G. (2024). Predictive analytics and ML in FinTech. In *AI and chatbots in FinTech* (pp. 41-54). Springer. https://doi.org/10.1007/978-3-031-55536-7_4
16. Aslam, M., Abbasi, M. A. K., Khalid, T., Shan, R. U., et al. (2022). Improving data security and privacy in smart cities. *Sensors, 22*(23), 9338. https://doi.org/10.3390/s22239338
17. Bader, A., Qtaish, A., Odeh, K., & Sa'd, H. (2025). Artificial intelligence and big data in accounting: The case of commercial banks in Jordan. *Al-Zaytoonah University Journal of Business, 1*(3), 1-18. https://doi.org/10.15849/zjjb.v1i03.49
18. Barelli, R., D'Onghia, M., & Longari, S. (2025). Toward secure electronic voting: A survey on E-voting systems and attacks. *IEEE Access, 13,* 89600-89626. https://doi.org/10.1109/ACCESS.2025.3569334
19. Bhatia, M. (Ed.). (2022). Cloud adoption. In *Banking 4.0* (pp. 129-146). Springer. https://doi.org/10.1007/978-981-16-6069-6_6
20. Campisi, G., Muzzioli, S., & De Baets, B. (2024). Predicting U.S. stock market direction. *International Journal of Forecasting, 40*(3), 869-880. https://doi.org/10.1016/j.ijforecast.2023.07.002
21. Çera, G., Khan, K. A., & Solenički, M. (2024). Antecedents of mobile banking usage. *Global Business Review, 25*(5), 1150-1170. https://doi.org/10.1177/09721509211008686
22. Chang, C.-H. (2024). Exploring the effect of the government interventions on the information asymmetry in the post-pandemic. *Journal of Applied Business and Economics, 26*(6), 22-38. https://doi.org/10.33423/jabe.v26i6.7384
23. Chen, X., Wang, C., & Li, S. (2023). Supply chain finance and CSR. *Supply Chain Management, 28*(2), 324-346. https://doi.org/10.1108/SCM-10-2021-0478
24. Chen, Y., Wang, G.-J., Zhu, Y., Xie, C., & Uddin, G. S. (2024). Systemic risk drivers of FinTech institutions. *The European Journal of Finance, 30*(18), 2157-2190. https://doi.org/10.1080/1351847X.2024.2358940
25. D'Innocenzo, E., Lucas, A., Schwaab, B., & Zhang, X. (2024). Modeling extreme events. *Journal of Business & Economic Statistics, 42*(3), 903-917. https://doi.org/10.1080/07350015.2023.2260439
26. Endress, T. (2025). Financial inclusion in Southeast Asia. In T. Endress & Y. F. Badir (Eds.), *Business and management in Asia: Finance and investments in the digital age* (pp. 191-204). Springer. https://doi.org/10.1007/978-981-96-3452-1_12
27. Ghouse, S. M., Shekhar, R., & Chaudhary, M. (2025). Mobile wallet adoption in Oman. *Journal of Islamic Marketing, 16*(4), 1229-1257. https://doi.org/10.1108/JIMA-02-2024-0073
28. Giudici, P., Centurelli, M., & Turchetta, S. (2024). AI risk measurement. *Expert Systems with Applications, 235*, 121220. https://doi.org/10.1016/j.eswa.2023.121220
29. Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). PSD2 compliance and cybersecurity. *International Cybersecurity Law Review, 5*(1), 79-120. https://doi.org/10.1365/s43439-023-00108-8
30. Haq, I. U., Lee, B. S., Rizzo, D. M., & Perdrial, J. N. (2024). Automated ML for detecting anomalies. *Machine Learning with Applications, 16,* 100543. https://doi.org/10.1016/j.mlwa.2024.100543
31. He, P., Zhou, H., Jiang, C., Anand, A., & Zhou, Q. (2025). Responsible leadership and knowledge hiding. *Journal of Knowledge Management, 29*(1), 49-71. https://doi.org/10.1108/JKM-02-2023-0160
32. Heranval, A., Lopez, O., & Thomas, M. (2024). Bayesian credibility

http://dx.doi.org/10.21511/bbs.21(2).2026.19

and cyber insurance. *European Actuarial Journal, 14*(3), 749-776. https://doi.org/10.1007/s13385-024-00394-4

33. Idayani, R. W., Nadlifatin, R., Subriadi, A. P., & Gumasing, M. J. J. (2024). Cyber risk and FinTech. *Procedia Computer Science, 234*, 1356-1363. https://doi.org/10.1016/j.procs.2024.03.134

34. Jong, S. C., & Ong, D. E. L. (2024). A novel Bayesian network approach for predicting soil-structure interactions induced by deep excavations. *Tunnelling and Underground Space Technology, 152*, 105865. https://doi.org/10.1016/j.tust.2024.105865

35. Khader, M., Chai, W. X. T., & Neo, L. S. (2021). *Introduction to cyber forensic psychology: Understanding the mind of the cyber deviant perpetrators*. World Scientific. https://doi.org/10.1142/12164

36. Koop, G., McIntyre, S., Mitchell, J., & Poon, A. (2024). Using stochastic hierarchical aggregation constraints to nowcast regional economic aggregates. *International Journal of Forecasting, 40*(2), 626-640. https://doi.org/10.1016/j.ijforecast.2022.04.002

37. Lawrence, T. B., & Shadnam, M. (2008). Institutional theory. In W. Donsbach (Ed.), *The international encyclopedia of communication*. Wiley. https://doi.org/10.1002/9781405186407.wbieci035

38. Mahmud, I., Wei, J., & Summerfield, N. (2025). Mobile banking risk assessment. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2025.2503953

39. Meraj, M., Ishrat, I., & Kaur, M. (2025). FinTech adoption in UAE. *Qualitative Research in Financial Markets, 18*(3), 640-671. https://doi.org/10.1108/QRFM-02-2024-0024

40. Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems. *Journal of Risk and Financial Management, 18*(1), 41. https://doi.org/10.3390/jrfm18010041

41. Ndlovu, T., & Chikobvu, D. (2024). The GARCH-EVT-Copula approach to investigating dependence and quantifying risk in a portfolio of Bitcoin and the South African Rand. *Journal of Risk and Financial Management, 17*(11), 504. https://doi.org/10.3390/jrfm17110504

42. Niankara, I., Hassan, H. I., Traoret, R. I., & Islam, A. R. M. (2025). Consumer savings and digital remittance in open banking: Insights from bibliometric and geospatial econometric analysis. *Human Behavior and Emerging Technologies, 2025*(1), Article 9352257. https://doi.org/10.1155/hbe2/9352257

43. Oreqat, A. (2021). The degree of satisfaction of Facebook users about its features, usage motives and achieved gratifications: An applied study on students of the Faculty of Mass Communication at the Middle East University. *Middle East Journal of Communication Studies, 1*(1), Article 1. https://doi.org/10.71220/2585-001-001-001

44. Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S. K., Kshetri, N., & Eashrak, N. (2024). riskAIchain: AI-driven IT infrastructure-Blockchain-backed approach for enhanced risk management. *Risks, 12*(12), 206. https://doi.org/10.3390/risks12120206

45. Schetakis, N., Aghamalyan, A., Boguslavsky, I., Rees, H., Rakotomalala, S., & Griffin, L. (2024). Quantum machine learning for credit scoring. *Mathematics, 12*(9), 1391. https://doi.org/10.3390/math12091391

46. Shaban, O. S., & Omoush, A. (2025). AI-driven financial transparency and corporate governance: Enhancing accounting practices with evidence from Jordan. *Sustainability, 17*(9), Article 3818. https://doi.org/10.3390/su17093818

47. Shi, Y., & Jin, Y. (2025). How FinTech impacts urban economic resilience: Evidence from China. *Sustainability, 17*(17), 7717. https://doi.org/10.3390/su1717771

48. Sneha, Malik, P., Sharma, R., Ghosh, U., & Alnumay, W. S. (2023). Internet of Things and long-range antennas: Challenges, solutions and comparison in next-generation systems. *Microprocessors and Microsystems, 103*, 104934. https://doi.org/10.1016/j.micpro.2023.104934

49. Syarif, M. F., & Aysan, A. F. (2025). Enabling crowdfunding platforms in Qatar: A regulatory framework for growth and sustainable innovation based on network analysis and Monte Carlo simulation. *Journal of Islamic Marketing, 16*(3), 759-785. https://doi.org/10.1108/JIMA-05-2024-0196

50. Taqa, S. B. A. (2025). The mediating role of remote communication on the relationship between electronic human resource management practices and organizational performance in Iraqi commercial banks. *Middle East Journal of Communication Studies, 5*(1), 1-52. https://doi.org/10.71220/2585-005-001-001

51. Tawfik, O. I., Ahmed, M. A., & Elmaasrawy, H. E. (2024). The mediating role of mobile banking-based financial inclusion disclosure on the relationship between foreign investment and bank performance. *International Journal of Financial Studies, 12*(4), 128. https://doi.org/10.3390/ijfs12040128

52. Van Asselt, M. B., & Renn, O. (2011). Risk governance. *Journal of Risk Research, 14*(4), 431-449. https://doi.org/10.1080/13669877.2011.553730

53. Wu, M., Subramaniam, G., Li, Z., & Gao, X. (2025). Using AI technology to enhance data-driven decision-making in the financial sector. In S. Dixit, M. Maurya, V. Jain, & G. Subramaniam (Eds.), *Artificial intelligence-enabled businesses: How to develop strategies for innovation* (pp. 187-207). John Wiley & Sons. https://doi.org/10.1002/9781394234028.ch11

54. Xia, L., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle

with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society, 98*, 104771. https://doi.org/10.1016/j.scs.2023.104771

55. Ye, W., Chaiyapa, W., & Li, Y. (2024). A comparative study of energy governance on energy resilience: Process tracing of China and Thailand's solar power development. *Energy Strategy Reviews, 55*, 101500. https://doi.org/10.1016/j.esr.2024.101500

56. Zakki, M. N., Iftikhar, N., Khan, S. S. U., Nishat, F., & Arshi, O. (2025). Reviewing theoretical perspectives on IT governance and compliance in banking: Insights from U.S. regulatory frameworks. In F. Rehman, I. U. Khan, O. Arshi, & S. K. Gupta (Eds.), *Emerging trends in information system security using AI & data science for next-generation cyber analytics* (Vol. 32, pp. 119-133). Springer. https://doi.org/10.1007/978-3-031-81481-5_9

57. Zhang, X., Antwi-Afari, M. F., Zhang, Y., & Xing, X. (2024). The impact of artificial intelligence on organizational justice and project performance: A systematic literature and science mapping review. *Buildings, 14*(1), 259. https://doi.org/10.3390/buildings14010259

58. Zhao, M., & Park, H. (2024). Bidirectional risk spillovers between Chinese and Asian stock markets: A dynamic Copula-EVT-CoVaR approach. *Journal of Risk and Financial Management, 17*(3), 110. https://doi.org/10.3390/jrfm17030110

http://dx.doi.org/10.21511/bbs.21(2).2026.19