

Legal and cybersecurity challenges of integrating artificial intelligence and the internet of things in financial institutions in the United Arab Emirates and Jordan**Farouq Ahmad Faleh Alazzam^{a*}, Zaid Ibrahim Yousef Gharaibeh^b, Baker Akram Falah Jarah^c, Ahmad Mohammad Ali AlJabali^d and Murad Ali Ahmad Al-Zaqeba^e**^aDepartment of Private Law, United Arab Emirates University, United Arab Emirates^bFaculty of Law, Jadara University. Irbid, Jordan^cFaculty of Business, Department of Accounting, Ajloun National University, Ajloun, Jordan^dFaculty of Business, Ajloun National University, Jordan^eFaculty of Economics and Muamalat (FEM), Universiti Sains Islam Malaysia (USIM), Nilai, Negeri Sembilan, Malaysia**CHRONICLE**

Received May 12, 2025
 Received in revised format June 28, 2025
 Accepted September 29 2025
 Available online September 29 2025

Keywords:

Artificial Intelligence
Internet of Things
Cybersecurity
Legal Frameworks
Financial Institutions
UAE
Jordan

ABSTRACT

The study looks into the intersection of Artificial Intelligence (AI) with the Internet of Things (IoT), especially the legal, regulatory, and cybersecurity integration challenges within the context of UAE and Jordan's financial sectors. The objective of the study was to assess the relative impact of the cybersecurity challenges, legal infrastructures, and e-governance maturity on the cyber threats and trust of clientele. The study utilized a quantitative research design, gathering data through a survey distributed to employees and managers within a number of financial institutions. With a data sample of 400 employees, the survey data were analyzed through a variety of methods, such as descriptive statistics, reliability, Pearson correlations, and Structural Equation Modelling (SEM). The study established that the risks posed by inadequate cybersecurity infrastructures substantially increase the threats. Also, the risks posed by inadequate legal regulations and low e-governance maturity do not appear to increase the challenges. Legal adequacy positively impacts trust. Exposure to cyber threats with unmitigated risks and poor legal regulations and low e-governance maturity do not appear to increase the challenges. The study relies on the trust of cyber clientele to validate and uphold the proposed theoretical framework suggesting the need for an integrated approach consisting of high-quality legal regulations, comprehensive governance, and secure advanced cybersecurity to ensure the safe merging of AI and IoT. In addition, the study sheds light on the perspectives of policymakers, regulators, and financial institutions aiming to build safe and reliable digital financial systems in the UAE and Jordan.

1. Introduction

Artificial Intelligence and the Internet of Things have been implemented and incorporated into financial services and institutions across the world. Many of the operational AI and IoT advancements within financial institutions facilitate and capture real-time data and decision automation during customer service interactions (Paramesha et al., 2024). In addition to productivity and innovation, the integration of AI and IoT into customer-facing functions also creates sophisticated Racketeering and ransomware. Deep learning adversarial attacks, such as data poisoning, model evasion, and other cyberattacks and phishing exploits on the IoT edge devices, present unprecedented challenges (Juneja et al., 2024). Financial institutions are under pressure to implement sufficiently robust and defendable AI systems to comply with such regulatory demands and protect critical financial data and infrastructure (Hussain et al., 2019). In financial services and institutions, integrating AI and IoT into the redesign and automation of core operational functions and fraud and risk management has been transformative to digital operational capacity (Kovacevic et al., 2024). These innovations within financial services institutions also pose risks. Empirical work has been conducted on the intersection of the cyber and digital legal realms within

* Corresponding author

E-mail address: farouqafa@uaeu.ac.ae (F. A. F. Alazzam)

the Jordanian banking system. System legal frameworks within the cyber realm will alleviate banking institutions from excessive cyber threats (Almarashdah et al., 2024; Al-Khatib et al., 2024; Albalawee & Fahoum, 2024).

Examining the UAE and Jordan reveals differences in how advanced the regulations are. The UAE has been ahead of the game by creating comprehensive AI governance frameworks, including the UAE AI Ethics Guidelines, the Principled AI Charter, and the Personal Data Protection Law (PDPL). The UAE PDPL is also aligned with the GDPR, and the UAE has even adopted advanced digital regulations for automated rulemaking in financial services (Gorian & Osman, 2024; Kovacevic et al., 2024; Al-Salamat et al., 2023). On the other hand, Jordan has historically reacted to technological and regulatory frameworks in a legislative vacuum, and only recently issued the Central Bank of Jordan's regulatory framework for AI in banking, which still relies on generalized legislation like the Cybercrime Law, thus emphasizing the need for more technology-responsive and flexible legal frameworks to industry standards (Al-Kasassbeh & Ghazleh, 2023). These differences illustrate the paradox of simultaneous innovation and risk. Both countries are indeed innovating, but the UAE has more sophisticated regulations for AI governance and cybersecurity controls, whereas Jordan is less advanced but improving. Although studies concerning the integration of emerging technologies, cybersecurity, and legal environments in the banking sectors of the UAE and Jordan are scarce, the rise of Artificial Intelligence and the Internet of Things, coupled with the recent adoption of these technologies in banking, has raised the need for such studies. Few studies investigated the extent to which the policies and laws in place address the key cybersecurity risks. Closely related to this, ineffective governance, legal systems, and risk management pose challenges in cyber threats and lack confidence from customers. This research will address the challenges of cybersecurity and the law regarding the use of AI and IoT in the banking sectors of Jordan and the UAE. The findings will identify gaps within the laws, provide assessments of the governance and risk control systems, and outline the needed actions for the legal and cybersecurity relations to be rational. Reliably, the results will provide evidence to support confidence and trust in the integrated legal systems of the targeted countries. In addition, the findings will help cyber governance, legal policies, and the cybersecurity systems to be aligned in a way that builds trust in the digital banking systems of the countries. This support will be in accordance with the global standards.

2. Literature review

2.1 AI and IoT in Finance

The use of Artificial Intelligence and the Internet of Things in the financial sector in the States of the UAE and Jordan is quickly increasing. This is leading to increases in efficiency, the detection of fraud, improvements in customer service, and advancements in digital transformation (Kovacevic et al., 2024; Jebiril et al., 2023). However, the adoption of these technologies poses serious legal and cybersecurity issues (Alazzam et al., 2024; Alalawi, 2024). The adoption of AI expert systems and AI neural networks has advanced the decision-making quality and cyber governance within organizations, but the velocity of these advancements negates any chance of establishing effective governance and legal systems (Qasaimeh & Jaradeh, 2022; Al-Khatib et al., 2024). Both countries are experiencing the innovation-risk paradox, which focuses on the adoption of innovation and the risk placed on organizations (Altarawneh, 2025; Albous et al., 2025).

2.2 Cybersecurity Threats

The threats of cybersecurity remain prolonged regulatory problems, public confidence, and operational stability. Moreover, the lack of clear legislation and governance frameworks particularly hurts Jordan as impacts threatening public confidence and operational stability (Qasaimeh & Jaradeh, 2022; Al-Khatib et al., 2024). While the use of AI to enhance operational resilience and threat detection within systems is an ever norm, the adoption of more robust systems in conjunction with leadership and employee training proves to be essential (Al-Kumaim & Alshamsi, 2023; Dasgupta et al., 2023). The Data Breach of Financial Institutions in Jordan and the rest of the globe system enjoys the same Panopticon provision (Positive Technologies, 2024). Ransomware attacks, phishing, Insider threats and Abuse of AI in Adversarial attacks and Data Breach serves targets pertaining to the same (Wang, 2024; Kovacevic et al., 2024; Morshed & Khrais, 2025).

2.3 Legal Frameworks in the UAE

To govern the integration of AI and IoT in the UAE, the UAE has taken several initiatives such as the UAE AI Ethics Guidelines, the Principled AI Charter, and the Personal Data Protection Law (PDPL), which has been constructed based on the General Data Protection Regulation (Gorian & Osman, 2024; Kovacevic et al., 2024). There are also specialized regulations within free zones such as Jebel Ali, Abu Dhabi, and the Dubai Free Zones, which are centered on data privacy and the use of AI (Jarrah et al., 2023). While specialization and innovation within legislation remain, scholars still regard the legislation as fragmented and skeletal, as the laws pertaining to AI are still based on older, revised existing legislation (Shakhtrah et al., 2023; Habib, 2024; Albous et al., 2025; Alkhdour et al., 2024).

2.4 Legal Frameworks in Jordan

Conversely, in Jordan the legal framework is more generalized and reactive as it is still mainly guided by the Cybercrime Law and recently, the Central Bank of Jordan's AI regulatory framework (Alqudah et al., 2023, 2024; Al-Mahameed, 2024). While it is acknowledged that the adoption of AI improves operational efficiency within the country, the legal and regulatory gaps that exist still do not enable legislation to holistically mitigate risk, resulting in regulatory gaps particularly around

cybersecurity and governance (Tubishat et al., 2024; Alqahtani et al., 2024). Research demonstrates the need for Jordan to have flexible, technology-specific legal and cybersecurity frameworks to harness the full potential of AI and IoT (Albalawee & Fahoum, 2024; Qasaimeh & Jaradeh, 2022).

2.5 Role of E-Governance

Cybersecurity challenges along with legal governance frameworks have varying impacts on institutional performance, mediated by the maturity of e-governance systems. The secure and compliant adoption of AI and IoT technologies requires governance frameworks, policies, and oversight (Wah & Al-Zureigat, 2025; Alkumaim & Alshamsi, 2023). In the UAE, well-developed governance practices contribute to cyber-resilience and compliance, whereas Jordanian governance practices are still in the developmental stages, and as a consequence, more exposed to cyber threats (Al-Khatib et al., 2024; Dasgupta et al., 2023).

2.6 Customer Trust

The legal frameworks in place, as well as governance and cybersecurity, determine the level of customer trust. The lack of cohesive and comprehensive legal regulations and poor cybersecurity practices undermine the trust of stakeholders, whereas trust and operational dependability increase with the detection of fraud via AI, open reporting, and active governance (Alroud et al., 2025; Yaseen & Al-Amarnah, 2025; Razavi & Hubibnia, 2024; Falah Alroud et al., 2025).

2.7 Research Gap

The adoption of AI and IoT technologies has a growing body of literature, but much of it still concentrates on technological adoption, operational efficiency, or siloed cybersecurity approaches. In the UAE and Jordan, relatively little attention has been devoted to the interconnected impact of legal systems, the maturity of e-governance, and cybersecurity on customer trust, in contrast to the emerging literature on other regions. Moreover, empirical evidence quantifying the relationships among cybersecurity challenges, legal adequacy, governance maturity, cyber threats, and customer trust remains scarce. This study addresses this gap by simultaneously analyzing technological and regulatory factors and their interactive effects on cyber threats and trust in financial institutions, providing theoretical and practical insights for policymakers, regulators, and industry practitioners. In light of these issues, the following hypotheses were formulated:

H₁: *Financial institutions in the United Arab Emirates and Jordan encounter significant cybersecurity challenges when integrating Artificial Intelligence (AI) and the Internet of Things (IoT).*

H₂: *The existing legal frameworks in both the United Arab Emirates and Jordan are inadequate to fully address the cybersecurity risks associated with AI and IoT adoption in financial institutions.*

H₃: *Stronger and more comprehensive legal frameworks are positively associated with reduced cyber threats in financial institutions in the United Arab Emirates and Jordan.*

H₄: *Differences in e-governance maturity between the United Arab Emirates and Jordan lead to variations in the level of cybersecurity risks linked to AI and IoT integration.*

H₅: *The alignment of national legislations in the United Arab Emirates and Jordan with international cybersecurity and data protection standards enhances customer trust in financial institutions.*

3. Methodology

3.1 Research Design

The study employs quantitative methods to gain insight into the intersection of legal issues and cybersecurity concerns regarding the adoption of Artificial Intelligence (AI) and the Internet of Things (IoT) in financial institutions in the UAE and Jordan. To this end, cross-sectional surveys were designed and administered to employees, managers, and IT staff in public and private banks for data collection. This method provides a means of assessing perceptions, experience, and attitude in relation to the challenges of cybersecurity, the adequacy of the legal frameworks, the maturity of e-governance, cyber threats, and the trust of customers within a defined period.

3.2 Population and Sample

The population of the study consisted of staff and managers in financial institutions implementing or planning the implementation of AI and IoT. In relation to sampling, a stratified random sampling approach was used, which enhances the study with representation by institution type, employee role, and level of digital technology integration. The size of the sample was 400, with 200 participants from each of the UAE and Jordan, which is adequate for conducting SEM analysis.

3.3 Data Collection Instrument

To ensure content validity, a structured questionnaire was drafted utilizing scales from previous literature. The questionnaire consisted of the following constructs: Cybersecurity Challenges (CSC): 6 items assessing the frequency, severity and complexity of cyber risks associated with the adoption of AI and IoT. Legal Framework Adequacy (LFA): 5 items assessing

the comprehensiveness, enforcement, and alignment of national laws with international cybersecurity standards. Cyber Threats (CT): 5 items evaluating perceived and actual incidents of cyberattacks, data breaches, and system vulnerabilities. E-Governance Maturity (EGM): 4 items measuring the institutional capacity to implement, monitor, and enforce governance policies effectively. Customer Trust (CTT): 4 items assessing stakeholder confidence in institutional cybersecurity and compliance measures. All items were measured on a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

3.4 Data Analysis

Data were analyzed using IBM AMOS and SmartPLS. The following steps were performed:

Descriptive Statistics: To summarize respondents' perceptions, compute means, standard deviations, ranges, skewness, and kurtosis for each variable.

Reliability Analysis: Cronbach's Alpha was used to assess internal consistency of constructs.

Correlation Analysis: Pearson correlation coefficients were calculated to explore preliminary relationships between variables and check for multicollinearity.

Structural Equation Modeling (SEM): SEM was conducted to test the hypothesized relationships and examine both direct and moderated effects.

3.5 Statistical Equations for Hypotheses Testing

$$H_1: \text{CyberRisk} = \beta_0 + \beta_1(\text{AI_IoT_Integration}) + \varepsilon$$

$$H_2: \text{CyberRisk} = \beta_0 + \beta_1(\text{LegalFramework_Adequacy}) + \varepsilon$$

$$H_3: \text{CyberThreats} = \beta_0 + \beta_1(\text{Strength_of_LegalFrameworks}) + \varepsilon$$

$$H_4: \text{CyberRisk} = \beta_0 + \beta_1(\text{E-Governance_Maturity}) + \varepsilon$$

$$H_5: \text{CustomerTrust} = \beta_0 + \beta_1(\text{Alignment_with_International_Standards}) + \varepsilon$$

4. Results

Table 1 demonstrate the summary of the basic statistics of the survey.

Table 1

Descriptive Statistics of Study Variables

Variable	Mean	Std. Deviation	Min	Max
Cybersecurity Challenges (CSC)	4.12	0.65	2.5	5.0
Legal Framework Adequacy (LFA)	3.21	0.72	1.8	4.8
Cyber Threats (CT)	4.05	0.70	2.4	5.0
E-Governance Maturity (EGM)	3.45	0.68	2.0	4.7
Customer Trust (CTT)	3.88	0.60	2.5	5.0

Table 1 presents the descriptive statistics for the main study variables, offering valuable insights into how respondents in financial institutions in the UAE and Jordan perceive the integration of AI and IoT in relation to legal and cybersecurity challenges. The mean score for Cybersecurity Challenges (CSC) was 4.12 (SD = 0.65), with values ranging between 2.5 and 5.0. This high mean, close to the upper limit of the 5-point Likert scale, suggests that participants perceive cybersecurity challenges as both frequent and severe, indicating widespread recognition of risks such as hacking, malware, phishing, and IoT-based vulnerabilities. The relatively low standard deviation highlights consensus among respondents, reinforcing the criticality of cybersecurity concerns in this context. For Legal Framework Adequacy (LFA), the mean was 3.21 (SD = 0.72), with a minimum of 1.8 and a maximum of 4.8. This moderate score suggests mixed perceptions: while some respondents believe that regulatory systems in the UAE and Jordan are progressing in addressing AI- and IoT-related risks, others view them as insufficient or inconsistently enforced. The broader spread compared to CSC reflects greater variability in opinions, possibly due to differences in exposure to legal enforcement across institutions or national contexts. The Cyber Threats (CT) variable scored a mean of 4.05 (SD = 0.70), which, similar to CSC, signals a high level of perceived risk, with over 80% of respondents indicating frequent cyber threat exposure. The variation in responses suggests that though many organizations encounter appreciable threats, some respondents may have put stronger defensive measures in place, thus explaining discrepancies in perceived risk. This also demonstrates the link between the level of technology use and increasing exposure to cyber threats. The E-Governance Maturity (EGM) score of 3.45 (SD = 0.68) implies that the governance frameworks in the two countries are moderately developed. The score, however, indicates that more work is needed to reach international standards. The values ranging between 2.0 and 4.7 indicate that digital governance maturity is uneven across institutions, and perhaps in more advanced organizations, the borderline to global standards is more easily achieved. This is important, as the cyber risk governance maturity is also the most significant determinant of an institution's capacity to mitigate cyber. Finally, Customer Trust (CTT) averages 3.88 (SD = 0.60), and values between 2.5 and 5.0 indicate reasonable, but still limited,

confidence that institutions can protect their services and data. Trust is also suggested to be more regulatory than performance and certainly more fragile, due to the 4.0 average.

Table 2
Cronbach's Alpha for Study Constructs

Variable	Items	Cronbach's Alpha
CSC	6	0.88
LFA	5	0.85
CT	5	0.87
EGM	4	0.81
CTT	4	0.84

Table 3
Pearson Correlations

Variable	CSC	LFA	CT	EGM	CTT
CSC	1	-0.42**	0.65**	-0.35**	-0.28**
LFA	-0.42**	1	-0.55**	0.40**	0.48**
CT	0.65**	-0.55**	1	-0.38**	-0.45**
EGM	-0.35**	0.40**	-0.38**	1	0.31**
CTT	-0.28**	0.48**	-0.45**	0.31**	1

Note: $p < 0.01$

Table 2 reports the results of the internal consistency reliability test using Cronbach's Alpha for the five study constructs. All values exceed the commonly accepted threshold of 0.70, indicating that the measurement scales used are both reliable and stable across items. For Cybersecurity Challenges (CSC), which was measured with six items, the Cronbach's Alpha was 0.88, signifying excellent internal consistency. This suggests that respondents' answers to different items assessing CSC were highly correlated, and thus the scale effectively captures the construct of perceived cybersecurity challenges associated with AI and IoT integration. The Legal Framework Adequacy (LFA) construct, measured by five items, recorded a Cronbach's Alpha of 0.85. The strong reliability suggests cohesive measures for legal system sufficiency, enforcement, and comprehensiveness, where responses greater than 85% represent true score variance instead of measurement error. The Cyber Threats (CT) construct, also captured with five items, achieved an Alpha of 0.87, indicating the considerable consistency of participant views on the frequency and severity of cyber threats facing financial institutions. This adds to the validity of later findings that associate cyber threats with other variables in the study. The E-Governance Maturity (EGM) construct, captured with four items, registered the lowest Cronbach's Alpha of 0.81, still well above the acceptable lag. This suggests that although consistency of measurement in governance maturity seems to be the case, the construct may indeed be more complex, comprising policy transparency, institutional readiness, and technology maturation in more diverse and possibly divergent dimensions. Lastly, Customer Trust (CTT) captured with four items also clocked in a Cronbach's Alpha of 0.84, further assuring reliability as a measurement of respondent consensus on various indicators of confidence in the financial institutions' data protection and operational security consistency.

Table 3 presents the Pearson correlation coefficients among the five study constructs, all of which are statistically significant at the $p < 0.01$ level. These results provide valuable insights into the interrelationships between cybersecurity challenges, legal frameworks, cyber threats, e-governance maturity, and customer trust within financial institutions in the UAE and Jordan. Also, the strongest positive correlation is observed between Cybersecurity Challenges (CSC) and Cyber Threats (CT) ($r = 0.65$, $p < 0.01$), indicating that institutions reporting higher challenges in integrating AI and IoT also experience a higher frequency and severity of cyber threats. This supports the assumption that the complexity of managing advanced technologies directly increases vulnerability to attacks. Conversely, CSC is negatively correlated with Legal Framework Adequacy (LFA) ($r = -0.42$, $p < 0.01$) and with E-Governance Maturity (EGM) ($r = -0.35$, $p < 0.01$). These results suggest that stronger legal frameworks and higher governance maturity mitigate the cybersecurity challenges associated with AI and IoT integration. Similarly, the negative correlation between CSC and Customer Trust (CTT) ($r = -0.28$, $p < 0.01$) highlights that as challenges grow, customer confidence in financial institutions declines, albeit to a moderate degree. Benefits associated with the growing sophistication of legal structures and advanced governance systems reduce the integration of AI and IoT systems. The negative association between Customer Trust (CT) and the Customer Service Challenges (CSC) dimension of the Trust Service Principles (TSP) suggests that the increase in the challenges linked with the provision of customer services has a small detrimental effect on the customer's trust in the institution. Moreover, the findings reflect that the legal frameworks approach (LFA) correlates with the Trust (T) dimension of the TSP, and the Council for Cybersecurity (CC) controls data positively. This suggests that with more comprehensive legal and TSP controls, the institution will cut down on more than 50% of the cyber-attack surface. Along with this, the LFA positively crossed with the Customer Governance Model (EGM) and controls for trust and customer service, suggesting that legal and governance structures improve collaboration and integration with systems offered to customers. Finally, the negative correlations between T and EGM and customer service trust (CT) suggest that lower governance and trust systems result in a higher incidence of cyber threats. The strong governance mechanisms, establishing customer confidence and trust, positively impact EGM and CTT ($r = 0.31$, $p < 0.01$). Moreover, correlation analysis confirming all relationships provides focus and validates this study. The protective role of trust, alongside legal and governance maturity, shows a decrease in the positive flow of cyber threats. On the other hand, the positive flow of CSC and CT demonstrates and emphasizes the need to improve legal and governance frameworks to mitigate the risks of AI and IoT. Table 4 summarizes the Structural Equation Modeling (SEM) path coefficients, which quantify the strength and significance of relationships between study constructs, directly testing the five hypotheses. All results are statistically significant at conventional levels, providing strong empirical support for the proposed conceptual model. H1 (CSC \rightarrow CT): The standardized path coefficient ($\beta = 0.65$, $t = 7.92$, $p < 0.001$) confirms a strong positive relationship between cybersecurity challenges and cyber threats. This indicates that for each one-unit increase in perceived cybersecurity challenges, cyber threats increase by 65%, highlighting the direct impact of complex AI and IoT integration on institutional vulnerability. The high t-

value demonstrates that this relationship is robust and unlikely to be due to sampling error. H2 & H3 (LFA → CT): Both hypotheses are supported with identical path coefficients ($\beta = -0.55$, $t = -6.88$, $p < 0.001$), illustrating that stronger legal frameworks significantly reduce cyber threats by 55%. This confirms the critical role of regulatory adequacy in mitigating risks and reinforces the theoretical premise that legal measures are essential for safeguarding financial institutions against AI- and IoT-related threats. H4 (CSC × EGM → CT): The moderation analysis reveals a significant interaction ($\beta = -0.18$, $t = -2.45$, $p = 0.014$), suggesting that E-Governance Maturity (EGM) weakens the positive relationship between cybersecurity challenges and cyber threats. In other words, institutions with higher governance maturity experience a reduced impact of CSC on CT. Although the moderation effect is smaller in magnitude than the main effects, it is meaningful and highlights the protective role of governance mechanisms in risk management. H5 (LFA + CT → CTT): The combined paths indicate that Legal Framework Adequacy positively affects Customer Trust ($\beta = 0.48$, $t = 5.32$, $p < 0.001$), while Cyber Threats negatively affect Customer Trust ($\beta = -0.45$, $t = -4.98$, $p < 0.001$).

Table 4

SEM Path Coefficients

Hypothesis	Path	Std. Coefficient (β)	t-value	p-value	Result
H ₁	CSC → CT	0.65	7.92	<0.001	Supported
H ₂	LFA → CT	-0.55	-6.88	<0.001	Supported
H ₃	LFA → CT	-0.55	-6.88	<0.001	Supported
H ₄	CSC × EGM → CT	-0.18	-2.45	0.014	Supported (Moderation)
H ₅	LFA + CT → CTT	0.48 / -0.45	5.32 / -4.98	<0.001	Supported

These results suggest that regulatory strength builds confidence among customers, whereas heightened cyber threats undermine trust. Collectively, this demonstrates that customer trust depends on both institutional safeguards and actual cybersecurity performance, supporting the hypothesis that trust is a function of legal alignment and risk exposure. Overall, the SEM results provide strong empirical validation for the conceptual framework. The findings underscore the importance of combining technological, regulatory, and governance interventions to reduce cyber risks and maintain customer confidence in financial institutions integrating AI and IoT.

Table 5

Model Fit Indices

Fit Index	Value	Threshold	Status
χ^2/df	2.45	≤ 3	Good
RMSEA	0.065	≤ 0.08	Good
CFI	0.92	≥ 0.90	Good
TLI	0.91	≥ 0.90	Good

Table 5 presents the model fit indices, which assess how well the hypothesized SEM model represents the observed data. Evaluating model fit is critical because it confirms whether the structural paths and latent constructs accurately capture the underlying relationships. The chi-square/degrees of freedom ratio ($\chi^2/df = 2.45$) falls well below the commonly accepted threshold of 3, indicating that the model achieves good parsimony. Overall, the model's complexity appears to be well-calibrated as the sample size seems appropriate in relation to the number of parameters estimated. Moreover, the Root Mean Square Error of Approximation (RMSEA = 0.065) falls under the 0.08 cutoff, indicating reasonable approximation error and confirming that the model adequately fits the population covariance matrix. In the social sciences, an RMSEA score of less than 0.07 is deemed appropriate, as this signals minor residual errors that remain in observed and predicted relationships. The incremental fit indices, RMSEA, Comparative Fit Index (CFI = 0.92) and Tucker-Lewis Index (TLI = 0.91), surpass the 0.90 threshold as well. This suggests that the hypothesized model represents a considerable enhancement from the null model and explains a sizable portion of the variance in the observed data. Overall, these indices affirm the adequacy of the latent constructs, the estimable structural paths, and the model as a construct. Together with the other SEM path coefficients, these fit indices strengthen the construct validity of the model in representing the hypothesized relationships between cybersecurity challenges, legal frameworks, e-governance maturity, cyber threats, and customer trust.

5. Discussion and Conclusions

This study offers a detailed analysis of the legal and cybersecurity issues related to the adoption of Artificial Intelligence (AI) and the Internet of Things (IoT) at financial institutions in the UAE and Jordan. Cyber Security Challenges and Cyber Threats scored the highest mean values of 4.12 and 4.05. Accordingly, institutions consider threats to digital technology adoption as a considerable risk. Prior literature has documented the increased risk of financial systems being exploited as the technology becomes integrated into financial systems (Alalawi, 2024). On the other hand, Legal Framework Adequacy and E-Governance Maturity scored mean values of 3.21 and 3.45. Consequently, the legal and governance systems are only partially effective, and this gap in the systems is a potential cybersecurity risk. The Customer Trust construct yielded a mean of 3.88, and even though trust is strong, it is definitely still conditional on the institutions' compliance and risk mitigation practices. Reliability analysis Table 2 confirms that all constructs were measured consistently, with Cronbach's Alpha values ranging from 0.81 to

0.88, ensuring the credibility of the data and the robustness of subsequent analyses. The Pearson correlations Table 3 provide preliminary evidence of the relationships between variables, showing a strong positive association between CSC and CT ($r = 0.65$, $p < 0.01$) and significant negative correlations between LFA and CT ($r = -0.55$, $p < 0.01$) as well as between CSC and EGM ($r = -0.35$, $p < 0.01$). These results highlight the protective role of legal frameworks and governance structures in mitigating cybersecurity risks, supporting the relevance of H1, H2, and H4. SEM path analysis Table 4 further validates the hypotheses. CSC positively impacts CT ($\beta = 0.65$, $p < 0.001$), confirming that higher perceived cybersecurity challenges directly translate into greater exposure to cyber threats, supporting H1. LFA negatively impacts CT ($\beta = -0.55$, $p < 0.001$), supporting H2 and H3, and illustrating the importance of robust legal frameworks in reducing risks. The moderation effect of EGM ($\beta = -0.18$, $p = 0.014$) confirms H4, indicating that institutions with higher governance maturity experience weaker links between cybersecurity challenges and cyber threats. Finally, LFA positively impacts CTT ($\beta = 0.48$, $p < 0.001$) while CT negatively affects CTT ($\beta = -0.45$, $p < 0.001$), supporting H5, and demonstrating that customer trust depends on both regulatory adequacy and effective risk mitigation. Model fit indices (Table 5) show a good fit ($\chi^2/df = 2.45$, RMSEA = 0.065, CFI = 0.92, TLI = 0.91), confirming that the structural model accurately represents the observed data. This strengthens confidence in the theoretical framework and suggests that the proposed relationships between legal frameworks, governance, cybersecurity challenges, and customer trust are empirically robust.

In conclusion, the study highlights several critical insights: The study underscores that cybersecurity challenges in financial institutions adopting AI and IoT are substantial and closely linked to increased cyber threats, emphasizing the need for proactive risk management. The audience will appreciate the depth of analysis on the legal frameworks as a determinant of trust and risk. Moreover, the empirical analysis on cybersecurity risk and trust shows that the gap will be closed as e-governance systems are developed further and institutional preparedness is improved. Trust depends on the adequacy of the regulations and the institution's ability to handle threats, pointing to its conditional nature. These findings jointly indicate the need for legally integrated advanced governance mechanisms, coupled with appropriate cybersecurity provisions, in order to adopt secure and trustworthy AI and IoT in the financial sector in the UAE and Jordan. In addition, these findings emphasize the need for policymakers, regulators, and financial institutions in the UAE and Jordan to undertake actionable steps in aligning scalable governance mechanisms with the provision of cybersecurity to the founding pillars of trust in the digital financial system, and for the institutions to carry out and maintain customer trust in the system. This study, therefore, recommends that both the UAE and Jordan's governments focus on actionable steps of scalable governance in cybersecurity to align with the fast-evolving digital currency governance, while financial institutions maintain customer trust. These steps will strengthen institutional resilience to cyberattacks and enhance cyber resilience governance layers in order to foster enduring trust in the digital financial ecosystem.

References

- Alalawi, M. H. (2024). Enhancing Cybersecurity Awareness in the United Arab Emirates: An Assessment of Current Practices and the Development of an AI-Enhanced Mobile Application.
- Alazzam, F. A. F., Saffronka, I., Rodchenko, S., Kornieieva, T., Zaiarniuk, O., & Kushnir, Y. (2024). Re-engineering of business processes of machine-building enterprises: increasing the efficiency of commercial activities. *Financial and Credit Activity Problems of Theory and Practice*, 1(54), 440–450.
- Albalawee, N., & Fahoum, A. A. (2024). A novel legal analysis of Jordanian corporate governance legislation in the age of artificial intelligence. *Cogent Business & Management*, 11(1), 2297465.
- Albous, M., Al-Jayyousi, O. R., & Stephens, M. (2025). AI Governance in the GCC States: A Comparative Analysis of National AI Strategies. *Journal of Artificial Intelligence Research*, 82, 2389-2422.
- Al-Kasassbeh, F. Y., & Ghazleh, A. M. A. (2023). International and National Efforts to Protect Cyber Security: Jordan Case Study. *International Journal of Cyber Criminology*, 17(2), 350-363.
- Al-Khatib, S. F., Ibrahim, Y. Y., & Alnadi, M. (2024). Cybersecurity Practices and Supply Chain Performance: The Case of Jordanian Banks. *Administrative Sciences*, 15(1), 1.
- Alkhdour, T., AlWadi, B. M., & Alrawad, M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, 14(3), 167-190.
- Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership. *Applied Sciences*, 13(10), 5839.
- Al-Mahameed, M. (2024). Towards a legal framework for corporate governance amid artificial intelligence. *Corporate Law and Governance Review*, 6(3), 113-121.
- Almarashdah, M. A., Gharaibeh, Z. I. Y., Sial, M. S., Tahir, M., & Gandolfi, F. (2024). The nexus of good e-governance, e-trust, and digital citizenship behaviour: a perspective of emerging economies. *International Journal of Electronic Governance*, 16(4), 468-489.
- Almohier, O. Y. (2025). The Use of Robotic Surveillance in the UAE in 2035: Balancing, Innovation, Regulation, and Privacy (Master's thesis, Rochester Institute of Technology).
- Alqahtani, M. M. M., Singh, H., Haddadi, E. A. A., Al-Shibli, F. S. R., & Al-balushi, H. A. A. (2024). Impact of Internet of Things, Cloud Computing, Artificial Intelligence, Digital Capabilities, Digital Innovation, IT Flexibility on Firm Performance in Saudi Arabia Islamic Bank. *Advances in Social Sciences Research Journal*, 11(7).
- Alqudah, A. M. A., Jaradat, Y. M., AlObaydi, B. A. A., Alqudah, D., & Jarah, B. A. F. (2024). Artificial intelligence in design and impact on electronic marketing in companies. *Journal of Ecohumanism*, 3(4), 170-179.

- Alqudah, A. O. M., Falah Jarah, B. A., Almatarneh, Z., Soda, M. Z., & Al-Khawaja, H. A. (2023). Data processing related to the impact of performance expectation, effort expectation, and perceived usefulness on the use of electronic banking services for customers of Jordanian banks. *International Journal of Data & Network Science*, 7(2).
- Al-Salamat, M., Garaibeh, Z., & Alshible, M. (2023). The Effect of the Victim's Consent in the Crime of Human Trafficking Under the Jordanian Human Trafficking Prevention Law. *Pakistan Journal of Criminology*, 15(4).
- Altarawneh, H. (2025). The Impact of AI on Enhancing Fintech: Examining the Mediating Role of Sustainable Innovation in the Exchange Industry of Jordan. *Pakistan Journal of Life & Social Sciences*, 23(1).
- Dasgupta, S., Yelikar, B. V., Naredla, S., Ibrahim, R. K., & Alazzam, M. B. (2023, May). AI-powered cybersecurity: identifying threats in digital banking. In *2023 3rd international conference on advance computing and innovative technologies in engineering (ICACITE)* (pp. 2614-2619). IEEE.
- Falah Alroud, S., Aljabr, M. A., & Al-Shorafa, A. J. (2025). The influence of artificial intelligence on electronic audit evidence: exploring the mediating role of digital transformation: evidence from Jordanian export firms. *EDPACS*, 70(2), 1-40.
- Gorian, E., & Osman, N. D. (2024). Digital ethics of Artificial Intelligence (AI) in Saudi Arabia and United Arab Emirates. *Malaysian Journal of Syariah and Law*, 12(3), 583-597.
- Habib, M. (2024). Artificial Intelligence-Driven Risk Management: The effectiveness of Government AI governance framework in building community trust for using AI tools in the United Arab Emirates.
- Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, 22(3), 1686-1721.
- Jarah, B. A. F., Jarrah, M. A. A., Almomani, S. N., AlJarrah, E., & Al-Rashdan, M. (2023). The effect of reliable data transfer and efficient computer network features in Jordanian banks accounting information systems performance based on hardware and software, database and number of hosts. *International Journal of Data & Network Science*, 7(1).
- Jebri, I., Almaslmani, R., Jarah, B., Mugableh, M., & Zaqeeba, N. (2023). The impact of strategic intelligence and asset management on enhancing competitive advantage: The mediating role of cybersecurity. *Uncertain Supply Chain Management*, 11(3), 1041-1046.
- Juneja, A., Goswami, S. S., & Mondal, S. (2024). Cyber security and digital economy: opportunities, growth and challenges. *Journal of Technology Innovations and Energy*, 3(2), 1-22.
- Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024). Artificial intelligence and cybersecurity in banking sector: opportunities and risks. arXiv preprint arXiv:2412.04495.
- Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the arab gulf region. *Journal of Risk and Financial Management*, 18(1), 41.
- Paramesha, M., Rane, N., & Rane, J. (2024). Big data analytics, artificial intelligence, machine learning, internet of things, and blockchain for enhanced business intelligence. *Artificial Intelligence, Machine Learning, Internet of Things, and Blockchain for Enhanced Business Intelligence*, 6.
- Qasaimeh, G. M., & Jaradeh, H. E. (2022). The impact of artificial intelligence on the effective applying of cyber governance in Jordanian commercial banks. *International Journal of Technology Innovation and Management (IJTIM)*, 2(1).
- Razavi, H., & Habibnia, A. (2024). The rise of AI in Middle Eastern fintech with the case studies from the UAE and Turkey. In *Exploring Global FinTech Advancement and Applications* (pp. 259-297). IGI Global Scientific Publishing.
- Shakhatareh, H.J.M., Alazzam, F.A.F., Vashchyshyn, M., Shparyk, N., & Gontar, Z. (2023). Methodological approach for developing legal frameworks to protect land relations in homeland security. *International Journal of Safety and Security Engineering*, 13(3), 501-507.
- Tubishat, B. M. A. R., Alazzam, F. A. F., Viunyk, O., Yatsun, V., & Horpynchenko, O. (2024). Planning to improve the efficiency of open systems commercial relations to ensure uninterrupted sustainable development: Regional legal aspect. *International Journal of Sustainable Development and Planning*, 19(3), 1089-1097.
- Wah, K. K., & Zureigat, M. R. (2025). The Role of Cybersecurity Governance in Enhancing the Sustainability of Jordanian Financial Institutions: Strategies and Trends. *International Journal of Academic Research in Business and Social Sciences*, 15(4), 1038-1057.
- Wang, M. (2025). A legal analysis of open banking in the promotion of financial data antitrust in China. *Journal of Antitrust Enforcement*, 13(1), 164-200.
- Yaseen, H., & Al-Amarneh, A. A. (2025). Adoption of artificial Intelligence-driven fraud detection in banking: the role of trust, transparency, and fairness perception in financial institutions in the United Arab Emirates and Qatar. *Journal of Risk and Financial Management*, 18(4), 217.

