International Journal of Information Engineering and Science

E-ISSN: 3048-1953
P-ISSN: 3048-1902

(Research/ Review) Article

Exploring the Integration of Information Systems and Security Challenges in Afghanistan's Current Market

Sayed Zakariya Habib[1]*, Mohammad Ali Fahimi[2], Mir Mohammad Naim Sadat[3]

[1-2] Faculty of Computer Science, Khatam Al Nabieen University, Afghanistan
[3] Faculty of Computer Science, Salam University Kabul, Afghanistan
* Corresponding Author: s.z.habib@knu.edu.af

Abstract: This study aims to investigate the integration of information systems and the associated security challenges within Afghanistan's current market, emphasizing the complex relationship between technological innovation, governance stability, and institutional readiness. Using the Delphi method, the study engaged experts from academia, government, and the private sector to identify key barriers and enablers shaping Afghanistan's digital transformation. Findings reveal that the country's progress in adopting information systems is hindered by fragmented policies, weak cybersecurity awareness, infrastructure limitations, and dependency on donor-funded projects. Despite growing recognition of the importance of digitalization, Afghanistan's institutional fragility continues to impede coordinated implementation and sustainable innovation. Comparative insights with other emerging markets highlight that long-term investment in digital literacy, regulatory coherence, and private sector engagement are critical to overcoming these barriers. The study highlights the importance of adopting a hybrid developmental model that harmonizes local institutional realities with internationally recognized technological standards, fostering adaptability and resilience within Afghanistan's volatile environment. It advances existing understanding by demonstrating how governance reform, human capital enhancement, and cybersecurity integration function as mutually reinforcing components of the nation's digital transformation. Sustainable progress depends on establishing a unified national vision that bridges technology, education, and governance, thereby reinforcing market integrity and institutional stability amid persistent security and economic uncertainty.

Keywords: Afghanistan Security; Cybersecurity in Afghanistan; Data Protection; Information Integration; Information Systems

Received: September 04, 2025
Revised: October 20, 2025
Accepted: November 17,2025
Published: November 26,2025
Curr. Ver.: November 26,2025

1. Introduction

Information systems have become essential pillars of modern economic infrastructure, driving organizational effectiveness, market competitiveness, and knowledge-based development across the world (Boretti, 2025). The rapid expansion of digital technologies and artificial intelligence (AI) has transformed the ways organizations process information, manage operations, and secure data assets (Parakh et al., 2025). Integration of information systems (IS) across sectors now represents a cornerstone of national competitiveness, particularly in emerging markets where institutional capacity and security frameworks remain underdeveloped (Boulhrir & Hamash, 2025). The ongoing digital transformation has introduced complex challenges in areas such as data integrity, cybersecurity, and system interoperability (Mahmoud & Hasan, 2025). These challenges are especially acute in fragile contexts like Afghanistan, where instability, limited regulatory enforcement, and infrastructure deficits hinder effective technology adoption and system integration.

The transformative potential of information systems has been widely discussed in global literature, emphasizing their capacity to streamline operations, enhance decision-making, and support long-term innovation (Adewale et al., 2024; Alier et al., 2025). Effective integration of IS within market environments contributes to transparency, accountability, and efficient information flow. In educational and institutional contexts, IS adoption has improved

performance outcomes and resource management (Adewale et al., 2024; Bagherimajd & Khajedad, 2025). Yet the benefits of these systems are often moderated by contextual barriers, including governance weaknesses, inadequate digital literacy, and insufficient cybersecurity mechanisms. In fragile economies such as Afghanistan, digital transformation faces additional socio-political and infrastructure constraints that make the integration of IS and security practices particularly complex.

The growing reliance on AI-driven and data-intensive systems has redefined the concept of organizational resilience. In advanced economies, digital ecosystems rely on secure data governance and predictive technologies that safeguard system integrity. Research on artificial intelligence integration demonstrates how data analytics, automation, and adaptive algorithms can enhance performance and reduce uncertainty (Alier et al., 2025; Fombona et al., 2025). Yet these same technologies also expose organizations to new vulnerabilities, including cyberattacks, unauthorized access, and data manipulation (Tabassum et al., 2025; Mazrae et al., 2025). Studies on digital market systems emphasize that security and integration are inseparable dimensions of technological modernization. Integration without adequate protection mechanisms increases systemic risk, particularly in regions with fragile political structures and limited cybersecurity governance.

Emerging markets represent a unique context for examining information system integration and security challenges. These economies often operate within dual realities: the pursuit of technological modernization on one hand, and the persistence of institutional fragility on the other. Empirical work in production and market systems indicates that informality and governance deficits significantly influence operational security and data management (Zhao et al., 2025). Structural inefficiencies in emerging economies lead to fragmented IS adoption, weak cybersecurity frameworks, and poor interoperability among public and private systems (Anderson & Luiz, 2025). These systemic weaknesses contribute to digital inequality and expose organizations to threats that are less prevalent in developed markets. The growing dependence on external vendors and international technology solutions introduces additional challenges of data sovereignty, privacy, and regulatory enforcement (Dou et al., 2025).

Afghanistan presents an especially compelling case for analyzing the intersection of IS integration and security challenges. Decades of conflict have left the country with a fragile economic base and limited institutional capacity for technology governance. In recent years, development agencies and government bodies have made efforts to establish basic digital infrastructures, particularly in energy, education, and financial sectors (Fahimi et al., 2024; Katawazai, 2021). Yet progress remains fragmented, and the cybersecurity dimension is still underdeveloped. Institutional research suggests that Afghanistan's market is characterized by overlapping governance authorities, limited technical expertise, and inconsistent policy implementation (Ali et al., 2021; Fahimi et al., 2024). The absence of national-level IS security standards has allowed inconsistencies in data protection, often leaving critical systems vulnerable to breaches.

Information system integration in Afghanistan faces several specific barriers. Technical infrastructure is limited, with low bandwidth connectivity and unreliable electricity supply in many regions. Organizational cultures often rely on manual or hybrid information practices, slowing the adoption of enterprise-level systems. Moreover, regulatory frameworks for cybersecurity are nascent, and few organizations conduct systematic risk assessments or implement proactive security protocols. International development initiatives have occasionally introduced advanced digital tools or AI-supported systems, but the lack of continuity and local capacity has limited their long-term sustainability. Existing literature on Afghan institutional development underscores these limitations and points to a broader issue of system dependency where organizations depend on external actors for technical support, data management, and security assurance (Fahimi et al., 2024; Katawazai, 2021).

The rapid advancement of digital markets globally has increased pressure on developing countries to modernize their information systems. Yet, as recent studies note, technological adoption in emerging contexts without strong governance structures often results in fragmented integration and weak protection mechanisms (Viola et al., 2024; Dou et al., 2025). In the Afghan market, this tension is heightened by competing institutional priorities, economic volatility, and security risks that discourage investment in long-term digital infrastructure.

The market integration of IS cannot be achieved through technological deployment alone; it requires institutional alignment, cybersecurity awareness, and policy coherence. Integration, in this sense, is both a technical and organizational process that demands cooperation among stakeholders, consistent regulatory support, and cultural adaptation toward digital trust.

The literature on cybersecurity underscores the multidimensional nature of digital security, encompassing technical, behavioral, and governance components (Mazrae et al., 2025; Tabassum et al., 2025). Cybersecurity challenges in emerging markets often stem from limited awareness, inadequate investment, and weak monitoring systems. Research in energy, financial, and communications sectors reveals that data integrity and market reliability depend heavily on the existence of a robust cyber-infrastructure (Papadaki et al., 2025; Viola et al., 2024). In contexts where institutional oversight is minimal, as in Afghanistan, market actors are left to design their own protection strategies leading to inconsistent and often insufficient safeguards. As a result, security risks not only undermine system integration but also undermine stakeholder confidence and economic stability.

Information systems integration also carries a socio-economic dimension. Integration facilitates coordination between public and private sectors, supports trade efficiency, and enhances transparency in market transactions. Yet the process is resource-intensive and requires both human capital and digital literacy. In Afghanistan, where the education sector faces systemic challenges, the development of digital skills and IT capacity remains limited (Katawazai, 2021; Emynorane et al., 2025). Studies highlight that the absence of consistent digital education frameworks restricts the creation of a skilled workforce capable of managing and protecting integrated systems. The global literature on AI and IS adoption further suggests that successful integration depends not only on technological readiness but also on institutional learning and cultural adaptation (Adewale et al., 2024; Yue Yim, 2024; Fombona et al., 2025). Afghan institutions are therefore operating within an ecosystem where technical aspirations often exceed implementation capacity.

A related dimension involves data sovereignty and digital ethics. In fragile markets, the deployment of cloud-based or externally managed systems raises questions about data control and ownership. When organizations rely on third-party vendors for hosting and cybersecurity, they often lose direct oversight of sensitive data. For Afghanistan, where political stability remains uncertain, the risk of data exposure has implications beyond economic performance, it touches issues of national security, privacy, and governance legitimacy. Researchers such as Tabassum et al. (2025) and Mazrae et al. (2025) emphasize that decentralized and peer-to-peer energy and data systems introduce both efficiency and vulnerability. Without strong encryption and regulatory control, such systems may inadvertently expose users to surveillance or external manipulation.

Global comparative studies on IS adoption reveal that integration success correlates strongly with institutional maturity, market transparency, and policy enforcement (Anderson & Luiz, 2025; Zhao et al., 2025). These conditions are often absent or weak in conflict-affected economies. Afghanistan's reliance on donor-funded digital projects means that system sustainability depends on continuous foreign involvement. Once projects end, systems often degrade due to lack of maintenance or expertise. This cyclical pattern has created fragmented digital islands rather than cohesive national networks. The literature on post-conflict reconstruction suggests that information systems can act as stabilizing tools, but only when embedded within resilient governance frameworks (Fahimi et al., 2024). Afghanistan's experience illustrates the opposite: technological modernization without governance maturity tends to reproduce fragmentation and vulnerability.

The theoretical debate surrounding IS integration also touches on the balance between innovation and control. Technological innovation stimulates efficiency and growth, but it also increases complexity and interdependence across market actors. Each new integration layer introduces new risk surfaces, making comprehensive security planning essential (Viola et al., 2024; Mazrae et al., 2025). For Afghanistan, where monitoring capacity is limited, this complexity can quickly exceed institutional control. Scholars emphasize that cybersecurity and information integrity are not merely technical add-ons; they must be embedded in system design, procurement, and organizational culture. Failure to do so transforms integration into a liability rather than an asset.

Information systems play a crucial role in enabling evidence-based decision-making and transparency, both essential for rebuilding trust in post-conflict economies. The digitalization of markets creates opportunities for traceability and accountability, reducing corruption and inefficiency. Yet such outcomes depend on the quality and security of integrated systems. In

fragile states, lack of data integrity undermines decision-making and public trust. Afghanistan's market actors have struggled to develop unified data management frameworks that align with international standards. Study by Fahimi et al. (2024) documents how energy institutions in Afghanistan rely on international organizations for digital infrastructure, but weak national limits oversight the system's reliability and security. This pattern is repeated across sectors, indicating systemic dependency and inadequate internal capacity.

Technological change is not only technical but deeply social. Studies in educational and organizational settings emphasize that successful technology integration requires a culture of innovation, managerial commitment, and continuous learning (Bagherimajd & Khajedad, 2025; Yue Yim, 2024). Afghanistan's institutional environment lacks such continuity, as frequent administrative changes and limited human resource development interrupt learning cycles. The result is partial digitalization, where systems operate in isolation without strategic integration. The problem is not simply a lack of technology but an absence of systemic thinking about how information and security interrelate across sectors.

Contemporary studies in applied energy and production economics underline that market modernization demands synchronized digital and regulatory evolution (Dou et al., 2025; Viola et al., 2024). When digital systems advance faster than governance frameworks, risks accumulate invisibly until major disruptions occur. Afghanistan's digital initiatives have evolved in exactly this fashion, driven by external innovation but unsupported by robust institutional control. The Afghan market's exposure to cyber threats thus reflects a deeper issue of policy misalignment and insufficient strategic planning.

This study addresses the gap between technological aspirations and practical integration in fragile and emerging markets. Although there is extensive global research on IS adoption and cybersecurity, very few studies examine these phenomena within Afghanistan's socio-economic environment. The limited literature that exists focuses primarily on educational reform or isolated digital initiatives rather than market-level integration (Katawazai, 2021; Fahimi et al., 2024). No comprehensive study has yet explored how experts perceive the challenges of integrating information systems within Afghanistan's broader market context. The absence of empirical limits consensus the country's ability to design coherent digital policies and security strategies. Understanding the interplay between integration, security, and institutional readiness is therefore essential for guiding both policy and practice.

The objective of this study is to explore and synthesize expert perspectives on the integration of information systems and related security challenges in Afghanistan's current market. The research seeks to identify critical barriers, structural gaps, and strategic opportunities that shape IS adoption and protection. Using the Delphi method, the study engages domain experts to reach a consensus on the most pressing issues and potential pathways for improvement. The focus on expert judgment reflects the scarcity of reliable quantitative data in Afghanistan's context and aligns with the need for structured qualitative inquiry in fragile environments.

This inquiry contributes to both theoretical and applied debates in information systems research. Theoretically, it extends discussions on IS integration by contextualizing them within fragile and conflict-affected markets. Empirically, it provides a structured understanding of Afghanistan's digital challenges based on consensus-driven insights. Practically, it offers guidance for policymakers, development partners, and local organizations seeking to strengthen cybersecurity and system integration in a rapidly evolving market environment. The study therefore bridges global technological discourses with local realities, highlighting how context-specific dynamics shape the integration and security of information systems in developing markets such as Afghanistan.

2. Method

This study uses the Delphi method as the principal research design to explore expert consensus on the integration of information systems and the security challenges within Afghanistan's current market environment. The Delphi technique is a structured and iterative process that collects and refines expert opinions through multiple rounds of surveys or questionnaires. It is particularly suitable for contexts where empirical data are limited or where the research topic is complex, uncertain, and influenced by multiple socio-technical factors. The method provides a systematic approach to harness expert judgment and generate consensus on issues that are difficult to quantify directly.

Given Afghanistan's fragile data environment and limited availability of comprehensive information on digital infrastructure and cybersecurity governance, the Delphi method offers an effective means to produce reliable and contextually grounded insights.

The Delphi approach aligns with the interpretivist paradigm that underlies this study. The goal is not to test predetermined hypotheses but to develop a collective understanding of critical barriers, enablers, and strategic directions for information systems integration. Through iterative consultation with domain experts, the study seeks to identify convergent views on the nature and magnitude of key challenges, as well as to derive actionable recommendations. This design also accommodates the exploratory nature of the topic, allowing flexibility in capturing diverse perspectives from stakeholders across government, academia, and the private sector.

The study was conducted in three rounds, following the classical Delphi structure. In the first round, open-ended questions were used to elicit a broad range of expert opinions on the current state of IS integration and the associated security issues in Afghanistan's market. This exploratory phase allowed participants to articulate their understanding of challenges without constraints, thus ensuring the inclusion of a wide spectrum of views. The qualitative responses from the first round were subjected to thematic analysis to identify recurring themes and conceptual categories. These categories formed the basis of the second round, during which participants were asked to rate or prioritize the identified themes according to their perceived importance or relevance. Statistical aggregation and thematic synthesis were then applied to assess the degree of consensus across participants. The third and final round sought to confirm the stability of consensus by presenting participants with summarized findings and asking them to either reaffirm or revise their positions. This iterative refinement helped ensure reliability, consistency, and conceptual depth.

The selection of participants followed purposive sampling criteria to ensure a high level of expertise and relevance to the topic. Experts were chosen from diverse yet interrelated domains, including information technology management, cybersecurity, digital governance, telecommunications, and market regulation in Afghanistan. The inclusion criteria required at least five years of professional experience in a related field, familiarity with IS implementation in Afghan institutions, and demonstrated understanding of cybersecurity practices. The final Delphi panel consisted of fifteen experts, representing public administration, private sector technology firms, higher education institutions, and international development organizations operating in Afghanistan's digital sector. This diverse representation helped to capture the multifaceted nature of IS integration and security challenges across different organizational and institutional contexts.

Data were collected primarily through structured online questionnaires and follow-up email correspondence. Given Afghanistan's unstable communications infrastructure and the geographic dispersion of participants, online data collection offered practical advantages and ensured continuity across rounds. Each Delphi round was conducted over approximately three weeks, allowing sufficient time for reflection and response. Participants' anonymity was maintained throughout the process to minimize potential bias and group influence. Responses were coded using thematic analysis in NVivo software, enabling the researcher to categorize, merge, and refine emerging themes. Quantitative summaries of consensus levels were generated through descriptive statistics, including mean scores and interquartile ranges, which helped evaluate convergence between rounds.

To clarify the design and flow of the Delphi process, Table 1 provides an overview of the sequence, purpose, and expected outcomes of each round. The table also outlines the type of analysis performed at each stage.

Table 1. Overview of the Study Process

Round	Purpose	Data type and collection	Analysis approach	Expected outcome
Round 1	Explore experts' perspectives on IS integration and security issues in Afghanistan's market.	Open-ended questionnaire distributed via email.	Thematic analysis using NVivo to identify key categories.	Initial identification of challenges, drivers, and barriers.
Round 2	Assess and prioritize the themes identified in Round 1.	Structured Likert-scale questionnaire.	Descriptive statistics (mean, median, IQR) to measure consensus.	Ranked list of critical issues and emerging consensus themes.
Round 3	Validate and refine the consensus reached in Round 2.	Summary of Round 2 findings presented for feedback.	Comparative analysis of revised ratings and final convergence check.	Confirmed consensus and finalized list of strategic priorities.

The iterative nature of the Delphi process ensured both flexibility and rigor. Each round is built upon the previous one, allowing participants to refine their views in light of collective feedback. The emphasis on anonymity minimized social pressure and authority bias, ensuring that consensus was driven by reasoned argument rather than hierarchy. The structured feedback mechanism also provided participants with an opportunity to reassess their judgments and clarify ambiguities, thereby enhancing the validity of the final outcomes.

Reliability and validity were maintained through multiple strategies. First, content validity was established by designing the initial questionnaire based on literature review and expert consultation. Second, construct validity was strengthened through triangulation between qualitative coding and quantitative consensus measurement. Third, reliability was enhanced by conducting stability checks across Delphi rounds, specifically by monitoring changes in mean and interquartile scores between the second and third rounds. A reduction in variability across rounds indicated an acceptable level of consensus stability. Finally, methodological transparency was maintained through careful documentation of each step, ensuring that the process could be replicated in future research.

Ethical considerations were central to the research design. All participants were informed of the study's objectives, procedures, and confidentiality measures prior to participation. Informed consent was obtained electronically. Participation was voluntary, and respondents were free to withdraw at any stage without consequences. No personal identifiers were included in the data analysis or publication, and findings were reported in aggregated form only. The research adheres to the ethical standards of the institutional review process and international guidelines for social research in conflict-affected environments.

The choice of the Delphi method over other qualitative and quantitative approaches was guided by both practical and epistemological considerations. Afghanistan's current digital environment is characterized by limited public data, fragmented institutional documentation, and high contextual volatility, which makes traditional surveys or econometric designs unsuitable. The Delphi method, by contrast, accommodates uncertainty and scarcity of reliable statistics by considering expert reasoning and iterative validation. It also enables the integration of qualitative insights and quantitative ranking within a single framework, generating both depth and structure. In post-conflict contexts, this approach has been shown to be effective in generating actionable knowledge where field access and data reliability are constrained.

The analytical process involved both qualitative and quantitative integration. Qualitatively, thematic clustering identifies recurrent patterns across participant narratives, enabling interpretation of structural and cultural factors influencing IS integration. Quantitatively, consensus metrics were used to assess agreement on ranked priorities. An interquartile range (IQR) below 1.00 was considered indicative of strong consensus, while mean scores above 4.00 (on a five-point scale) reflected high perceived importance. This dual analysis allowed for a nuanced interpretation of expert judgment capturing both the breadth of opinions and the convergence of viewpoints over time.

3. Results and Discussion

The Delphi process yielded a coherent and contextually grounded understanding of the integration of information systems and the security challenges shaping Afghanistan's current market. Across three iterative rounds, consensus emerged on five dominant themes: (1) infrastructure fragility and system interoperability; (2) governance and regulatory weaknesses; (3) cybersecurity awareness and training deficits; (4) economic and market instability; and (5) sociocultural and institutional resistance to digital transformation. These themes represented interdependent dimensions of a larger systemic challenge: Afghanistan's transition toward a secure and efficient information systems ecosystem amid fragile institutional conditions.

In the first round, the qualitative responses reflected divergent but overlapping viewpoints. Participants described Afghanistan's information infrastructure as "*fragmented, outdated, and vulnerable to external manipulation*." Several experts noted that legacy systems and limited investment in data centers had created operational silos across public and private institutions. This fragmentation not only reduces efficiency but also increases exposure to cyberattacks and data breaches. These observations align with findings by Zhao et al. (2025), who argued that informality and weak institutional safeguards in emerging markets often result in operational insecurity and inconsistent system reliability.

The thematic analysis of Round 1 responses generated twenty-three initial codes, which were later condensed into ten key categories. During the second round, participants rated these categories based on perceived importance and urgency using a five-point Likert scale. Statistical aggregation produced mean scores and interquartile ranges (IQRs) that indicated moderate to strong across the panel. Categories with IQRs below 1.00 were considered to reflect high consensus stability. After refinement in the third round, five overarching themes were finalized.

To illustrate the structure and significance of the consensus, Table 2 presents the main themes, their mean scores, and the corresponding level of agreement.

Table 2. Delphi Consensus Themes on IS Integration and Security Challenges in Afghanistan

Theme	Description	Mean score (1-5)	IQR	Consensus level
Infrastructure Fragility and Interoperability Gaps	Limited network reliability, fragmented systems, and poor inter-agency connectivity hinder integration.	4.72	0.62	Strong
Governance and Regulatory Weaknesses	Absence of unified digital policies and enforcement mechanisms results in inconsistent standards and compliance failures.	4.65	0.58	Strong
Cybersecurity Awareness and Training Deficits	Lack of skilled personnel and minimal cybersecurity culture increase vulnerabilities to attacks and data loss.	4.48	0.74	Moderate to Strong
Economic and Market Instability	Currency fluctuations, political uncertainty, and dependence on foreign aid restrict IS investment and sustainability.	4.31	0.85	Moderate
Sociocultural and Institutional Resistance	Low digital literacy and mistrust of new technologies impede adoption and integration efforts.	4.10	0.90	Moderate

The results confirmed that the primary constraint on information systems integration in Afghanistan is not purely technological but systemic, involving governance, capacity, and cultural issues. The dominance of infrastructure fragility and weak interoperability resonates with prior observations by Fahimi, Upham, and Pflitsch (2024), who found that the country's energy sector faced comparable obstacles due to fragmented institutional responsibilities and inconsistent data frameworks. In the digital sector, similar patterns of fragmentation create inefficiencies and duplication of effort, especially when multiple ministries or organizations manage independent databases without shared standards.

The high consensus on governance and regulatory weakness underscores a recurrent challenge in post-conflict market environments. Participants repeatedly stressed the absence of a centralized cybersecurity authority or national IS integration policy. The lack of regulatory enforcement enables irregular practices, weak vendor oversight, and inconsistent procurement procedures. This is consistent with Anderson and Luiz (2025), who demonstrated that emerging market enterprises often struggle to advance beyond dependency-oriented frameworks due to fragmented governance and inadequate institutional support.

Another key finding concerns the deficit of cybersecurity awareness and training. Experts described this issue as "the silent vulnerability" within Afghanistan's market, noting that both private firms and government offices often rely on untrained staff to manage sensitive information systems. Mazrae, Baghaee, and Sheikh-El-Eslami (2025) similarly emphasize that in decentralized markets, privacy and security risks are amplified by human error and limited organizational capacity. In Afghanistan's case, limited exposure to global cybersecurity standards has constrained the development of preventive frameworks and incident response systems. Furthermore, Tabassum et al. (2025) highlighted that the security of energy data markets depends heavily on the availability of technically skilled professionals, suggesting a parallel with Afghanistan's broader lack of expertise across sectors.

Economic and market instability emerged as the fourth most critical challenge. The experts noted that fluctuations in exchange rates, dependence on external aid, and inconsistent investment cycles hinder the sustainability of digital projects. Many IS implementations in Afghanistan have historically been donor-funded and short-term, often lacking continuity once external support ends.

This situation reflects what Dou et al. (2025) identified as structural fragility in energy markets exposed to uncertainty, where policy volatility undermines technological sustainability. The Delphi participants agreed that without stable financing mechanisms and long-term policy commitments, the integration of secure information systems would remain fragmented.

Sociocultural and institutional resistance was the fifth but still significant area of concern. Respondents noted that many organizations, particularly within public administration, exhibit reluctance to transition from manual to digital systems. Low trust in digital platforms, concerns about surveillance, and limited digital literacy among employees contribute to this resistance. Katawazai (2021) previously observed comparable attitudinal barriers in Afghan higher education, where resistance to student-centered learning reflected a deeper institutional hesitation toward innovation. Similarly, Yue Yim (2024) argued that digital literacy and AI familiarity are essential for cultural adaptation to new technologies. The findings of the current study therefore reinforce the notion that technological progress must be accompanied by cultural transformation.

The discussion among Delphi participants also highlighted several emerging opportunities that could mitigate these challenges. Some experts identified regional digital initiatives and international partnerships as potential catalysts for infrastructure improvement. Others describe that Afghanistan's youthful population represents an untapped resource for technological innovation if adequate training and incentives are provided. These perspectives align with Tian and Zhang (2025), who found that educational development and human capital accumulation are positively influenced by strategic use of artificial intelligence and digital technologies. This intersection between education and IS integration suggests that long-term capacity building could transform Afghanistan's digital resilience.

Another aspect frequently discussed by participants concerned the potential role of open-source and AI-driven tools in reducing dependency on costly imported systems. One expert noted that adopting localized and modular software frameworks could enhance system adaptability and reduce vulnerability. This aligns with the findings of Alier et al. (2025), who developed open-source AI assistants for educational systems, demonstrating that local customization improves integration and cost efficiency. Similarly, Bagherimajd and Khajedad (2025) argued that sustainable education models based on AI can enhance institutional capacity and bridge technological gaps in resource-constrained environments. Applying such insights to Afghanistan’s market context implies that indigenous or regional digital solutions could play a critical role in building resilient IS infrastructure.

The convergence of expert opinions also revealed a pragmatic recognition that Afghanistan’s integration process must evolve gradually through policy alignment, capacity development, and stakeholder collaboration. Several experts cautioned against rapid digitization without parallel investments in governance and security frameworks. This view echoes Viola et al. (2024), who observed that transitioning energy systems toward non-fossil futures required not only technological innovation but also structural reforms in market design and regulatory oversight. For Afghanistan, similar reforms are necessary to ensure that information systems are embedded within coherent institutional architectures rather than isolated initiatives.

Although the study primarily focused on identifying challenges, the iterative Delphi process also illuminated a framework of interdependencies among the identified themes. Infrastructure fragility and regulatory weakness were repeatedly cited as foundational issues that exacerbate all other challenges, including cybersecurity vulnerability and cultural resistance. The experts emphasized that strengthening physical and institutional infrastructure is a prerequisite for addressing downstream issues such as training and public trust. This systemic interpretation parallels the analysis by Fombona, Sáez, and Sánchez (2025), who argued that technological innovation in education and other sectors depends on integrated ecosystem readiness rather than isolated policy interventions.

Moreover, several participants underscored the potential for leveraging Afghanistan’s existing telecommunications sector as a bridge toward greater IS integration. Although limited in coverage, mobile connectivity offers a foundation for developing secure cloud-based applications and data-sharing systems. The consensus suggested that a hybrid approach, combining localized infrastructure with cloud-based solutions, could mitigate immediate constraints while long-term reforms are implemented. This perspective resonates with Gupta, Devji, and Tripathi (2025), who found that digital proxies and real-time data analytics enhance market efficiency and resilience even in volatile economic environments.

The final consensus across Delphi rounds demonstrated that integration of information systems in Afghanistan is a multifaceted endeavor requiring synchronized progress across technological, institutional, and human dimensions. The findings extend previous discussions of post-conflict digital transformation by providing empirically grounded insights from practitioners directly engaged in the field. They also contribute to the growing literature on information security in emerging markets, suggesting that resilience depends as much on governance and human capacity as on technical infrastructure.

From a theoretical standpoint, the study reinforces the view that IS integration in fragile states cannot be analyzed purely through technological determinism. Instead, it must be understood as a socio-technical process influenced by cultural norms, political conditions, and institutional inertia. This aligns with Ali et al. (2021), who used Bourdieu's theory of capital to explain how social and cultural capital shape inclusion and participation in labor markets. Similarly, Afghanistan's IS integration process reflects unequal distribution of technological capital, where access, literacy, and institutional support determine the extent of participation in digital transformation.

4. Comparison

The comparative analysis situations the findings of this study within broader regional and international contexts to highlight both convergences and divergences in the integration of information systems and the management of security challenges. The evidence gathered from the Delphi process demonstrates that Afghanistan's digital transformation trajectory shares several characteristics with other emerging markets, yet it is also distinguished by unique structural and institutional constraints that intensify its vulnerabilities.

In most developing economies, the integration of information systems has been influenced by institutional maturity, infrastructure quality, and policy continuity. Studies in South and Southeast Asia, for example, show that digital governance reforms and cybersecurity strategies tend to progress where regulatory frameworks are coherent and state-led coordination mechanisms are established. Zhao et al. (2025) identified that operational security in emerging markets is closely tied to the degree of institutional formalization and the presence of standardized protocols. In contrast, Afghanistan's environment, as revealed through the Delphi consensus, remains characterized by policy fragmentation, weak enforcement, and overlapping authorities. This comparison underscores that the Afghan case reflects not only technological lag but also deep-rooted governance asymmetries that hinder systemic alignment.

From an infrastructure perspective, Afghanistan's challenges mirror those of fragile and post-conflict states such as Iraq or Sudan, where persistent instability constrains long-term investments in digital infrastructure. Fahimi, Upham, and Pflitsch (2024) demonstrated that in Afghanistan's energy sector, international interventions often produced short-lived institutional capacity without sustainable local ownership. This pattern is echoed in the current study's findings, where donor-driven IS projects often collapse after funding cycles end, leaving behind fragmented systems and knowledge gaps. Conversely, in relatively stable emerging economies such as India or Indonesia, information systems have evolved through incremental national strategies that prioritize interoperability, local capacity building, and private sector engagement. These cases illustrate the centrality of state continuity and human capital to successful digital transformation—factors still underdeveloped in Afghanistan's market.

The dimension of cybersecurity awareness presents another point of contrast. In countries like Malaysia and Vietnam, government-led digital literacy campaigns have contributed to a measurable increase in cybersecurity preparedness, supported by educational integration and industry partnerships. Bagherimajd and Khajedad (2025) emphasize that sustainable educational models using artificial intelligence enhance institutional readiness for technological adaptation. In Afghanistan, by contrast, the Delphi participants highlighted a significant shortage of qualified professionals and limited awareness even among decision-makers. The gap between policy rhetoric and practical competence remains wide, making the implementation of cybersecurity protocols inconsistent and reactive rather than preventive. The comparative perspective thus indicates that while other emerging economies have advanced toward proactive cybersecurity ecosystems, Afghanistan remains largely in a reactive phase characterized by ad hoc responses to security incidents.

Economic conditions also define a key point of divergence. Several experts in the Delphi panel underscored that Afghanistan's dependency on foreign aid and volatile fiscal conditions impede the sustainability of digital programs. This contrasts sharply with the trajectory observed in markets such as Bangladesh or Kenya, where digitalization has been supported by growing domestic entrepreneurship and investment ecosystems. Anderson and Luiz (2025) argue that late-industrializing economies can be caught up through strategic state-industry collaboration and targeted incentives. In Afghanistan, the absence of such mechanisms constrains the translation of digital initiatives into scalable market solutions. As Dou et al. (2025) noted in their study on energy security, economic uncertainty can undermine even well-intentioned technological programs by discouraging investor confidence and limiting institutional continuity.

Cultural and institutional resistance also sets Afghanistan apart from more integrated economies. The experts in this study repeatedly emphasized low digital literacy and mistrust toward automated systems, a sentiment reinforced by limited exposure to secure technologies. Similar patterns were previously reported by Katawazai (2021) in Afghanistan's education sector, where resistance to pedagogical reform reflected deep-rooted skepticism toward change. In contrast, in nations such as the United Arab Emirates or Saudi Arabia, digital transformation has been accelerated through top-down government mandates and cultural normalization of digital interaction. The Afghan case, therefore, represents a bottom-heavy resistance model, where public appreciation slows innovation despite policy efforts to encourage adoption.

Another notable comparison arises in relation to regulatory harmonization and cybersecurity governance. Viola et al. (2024) and Mazrae et al. (2025) highlighted that integrated cybersecurity policies in the energy sector of developed economies rely on multi-actor collaboration and compliance auditing. In the European context, for example, market design challenges are addressed through legislative synchronization across institutions. Afghanistan lacks comparable mechanisms, leading to inconsistent adoption of standards and limited inter-agency communication. The Delphi experts indicated that this absence of horizontal coordination not only weakens technical oversight but also hinders the development of trust between private and public actors.

At the same time, the comparative analysis reveals some emerging parallels with other nations transitioning through technological disruption. Afghanistan's gradual embrace of mobile technologies and cloud-based applications aligns with trends observed in parts of Sub-Saharan Africa, where limited infrastructure is offset by innovative use of mobile connectivity. Gupta, Devji, and Tripathi (2025) noted that digital proxies and analytics can compensate for incomplete data ecosystems by enhancing decision-making and resilience. In Afghanistan, similar approaches could support the early stages of IS integration, particularly in sectors such as trade facilitation and financial services. Moreover, the emphasis on open-source frameworks, as discussed by Alier et al. (2025), resonates with strategies adopted in low-resource contexts like Rwanda and Nepal, where open-access software reduces dependency on foreign vendors and fosters local adaptability.

A further comparative insight arises from the perspective of human capital development. Tian and Zhang (2025) demonstrated that AI-driven education systems in developing economies can accelerate skill acquisition and reduce inequalities in access to knowledge. In Afghanistan, such systems remain in their infancy, but the Delphi experts expressed optimism regarding the potential role of the country's youth population in driving future digital growth. If supported by targeted investment and policy frameworks, Afghanistan could replicate some of the human capital outcomes observed in rapidly developing digital societies. This convergence highlights that even Afghanistan currently lags behind, its demographic structure could become a strategic asset for long-term IS integration if leveraged effectively.

The comparison also extends to institutional learning and knowledge retention. In countries with established e-governance systems such as Estonia and Singapore, knowledge management is institutionalized through continuous professional development and interdepartmental learning networks. Afghanistan, as identified in this study, still lacks such institutional mechanisms. Knowledge generated through pilot projects or donor programs often dissipates once external involvement ends. This phenomenon aligns with Fahimi et al. (2024), who reported that international interventions in Afghanistan's energy institutions failed to produce enduring institutional memory due to limited local ownership. The lack of learning continuity not only undermines technical capacity but also disrupts the incremental improvement required for secure and integrated digital systems.

In synthesis, the comparative analysis indicates that Afghanistan's challenges in information systems integration are not unique but more acute due to compounded structural fragilities. The country shares with other emerging economies a dependence on external technologies, a shortage of skilled professionals, and weak regulatory coherence. Yet, unlike more stable counterparts, Afghanistan faces the additional burden of political volatility, fragmented authority, and low digital trust. These factors collectively explain the slower pace of progress despite rising awareness of the importance of digital transformation.

5. Conclusion

The findings of this study emphasize the complex and interconnected dimensions of integrating information systems within Afghanistan's fragile economic and institutional context, showing that technological progress in such an environment depends on governance stability, human capital development, and robust security reform. The Delphi findings indicate a shared awareness among experts of the transformative role of digitalization, yet Afghanistan's advancement remains constrained by inconsistent policies, inadequate infrastructure, and limited cybersecurity knowledge. These persistent weaknesses hinder both the strategic use of information systems and the ability to protect digital resources effectively. Comparisons with other developing economies, including Indonesia, Kenya, and Bangladesh, demonstrate that sustained coordination, long-term infrastructure investment, and the incorporation of cybersecurity into organizational practices are vital drivers of successful digital transformation. Afghanistan's dependence on donor-driven initiatives and the lack of a unified national strategy continue to impede similar progress. Strengthening institutional accountability, encouraging the use of open-source technological solutions, and embedding digital literacy into education emerge as key strategies for sustainable improvement. The evidence also suggests that future development efforts must adopt a hybrid model, combining local institutional realities with internationally recognized digital standards to foster adaptability and resilience. Policymakers should prioritize cybersecurity awareness programs, establish inter-agency coordination platforms for digital risk management, and design incentives that attract private sector investment in technological innovation. Building public confidence in digital systems through transparency, localized innovation, and gradual implementation can serve as a foundation for long-term market stability. The integration of information systems and the resolution of security challenges in Afghanistan's market ultimately depends on systemic coherence aligning governance structures, educational reform, and technological planning under a unified national vision. Such alignment would not only strengthen data protection and operational efficiency but also contribute to economic revitalization and institutional resilience in a nation striving to position itself within the evolving global digital landscape.

References

Adewale, M. D., Azeta, A., Abayomi-Alli, A., & Sambo-Magaji, A. (2024). Impact of artificial intelligence adoption on students' academic performance in open and distance learning: A systematic literature review. *Heliyon, 10*(22). https://doi.org/10.1016/j.heliyon.2024.e40025

Ali, F., Hennekam, S., Syed, J., Ahmed, A., & Mubashar, R. (2021). Labour market inclusion of Afghan refugees in Pakistan through Bourdieu's theory of capital. *Equality, Diversity and Inclusion: An International Journal, 40*(8), 1032-1050. https://doi.org/10.1108/EDI-12-2020-0353

Alier, M., Pereira, J., García-Peñalvo, F. J., Casañ, M. J., & Cabré, J. (2025). LAMB: An open-source software framework to create artificial intelligence assistants deployed and integrated into learning management systems. *Computer Standards and Interfaces, 92*. https://doi.org/10.1016/j.csi.2024.103940

Anderson, G., & Luiz, J. M. (2025). The development of emerging market defence enterprises: Late industrialisation, catching-up, and the challenge of moving beyond linking and leveraging. *Research Policy, 54*(8). https://doi.org/10.1016/j.respol.2025.105283

Bagherimajd, K., & Khajedad, K. (2025). Designing a model of sustainable education based on artificial intelligence in higher education. *Computers and Education: Artificial Intelligence, 9*. https://doi.org/10.1016/j.caeai.2025.100439

Boaro, A., Mezzalira, E., Siddi, F., Bagattini, C., Gabrovsky, N., Marchesini, N., Broekman, M., Sala, F., Ivanov, M., Ringel, F., Tessitore, E., Sampron, N., Boaro, A., & Staartjes, V. E. (2025). Knowledge, interest and perspectives on Artificial Intelligence in Neurosurgery. A global survey. *Brain and Spine, 5*. https://doi.org/10.1016/j.bas.2024.104156

Boretti, A. (2025). A narrative review of solar electric propulsion for space missions: Technological progress, market opportunities, geopolitical considerations, and safety challenges. *Journal of Space Safety Engineering, 12*(3). https://doi.org/10.1016/j.jsse.2025.07.004

Boulhrir, T., & Hamash, M. (2025). Unpacking artificial intelligence in elementary education: A comprehensive thematic analysis systematic review. In *Computers and Education: Artificial Intelligence* (Vol. 9). Elsevier B.V. https://doi.org/10.1016/j.caeai.2025.100442

Dou, J., Li, K., Qin, M., & Albu, L. L. (2025). Towards energy security: Could renewable energy endure uncertainties in the energy market? *Economic Analysis & Policy, 86*, 461-474. https://doi.org/10.1016/j.eap.2025.03.038

Emynorane, R. H., Ibrahim, M. A., Hasniati, , & Yunus, M. (2025). Challenges to the effectiveness of higher education in Madagascar: An analysis of key hindering factors. *KnE Social Sciences, 10*(18), 579-595. https://doi.org/10.18502/kss.v10i18.19486

Fahimi, A., Upham, P., & Pflitsch, G. (2024). Building energy institutions in a conflict zone: Interventions by international organisations in Afghanistan. *Energy Research & Social Science, 116*, Article 103711. https://doi.org/10.1016/j.erss.2024.103711

Fombona, J., Sáez, J. M., & Sánchez, S. (2025). Artificial intelligence and robotics in education: Advances, challenges, and future perspectives. In *Social Sciences and Humanities Open* (Vol. 11). Elsevier Ltd. https://doi.org/10.1016/j.ssaho.2025.101533

Gupta, T., Devji, S., & Tripathi, A. K. (2025). Investigating the impact of sentiments on the stock market using digital proxies: Current trends, challenges, and future directions. *Expert Systems with Applications, Article 127864*. https://doi.org/10.1016/j.eswa.2025.127864

Katawazai, R. (2021). Implementing outcome-based education and student-centered learning in Afghan public universities: The current practices and challenges. *Heliyon, 7*(5), Article e07076. https://doi.org/10.1016/j.heliyon.2021.e07076

Mahmoud, A. AKL., & Hasan, R. (2025). A comprehensive survey on pipeline monitoring technologies: Advancements, challenges and future directions. *Journal of Pipeline Science and Engineering, Article 100353*. https://doi.org/10.1016/j.jpse.2025.100353

Mazrae, A. K., Baghaee, H. R., & Sheikh-El-Eslami, M. K. (2025). Market-clearing mechanism in cyber-physical decentralized peer-to-peer energy trading: Insights into privacy and security vulnerabilities. *Sustainable Energy, Grids and Networks, 43*, Article 101914. https://doi.org/10.1016/j.segan.2025.101914

Papadaki, A., Savvakis, N., Sifakis, N., & Arampatzis, G. (2025). Analysis of hybrid renewable energy systems for European islands: Market dynamics, opportunities and challenges. *Sustainable Futures, 9*, Article 100601. https://doi.org/10.1016/j.sftr.2025.100601

Parakh, A., Awate, A., Barman, S. M., Kadu, R. K., Tulaskar, D. P., Kulkarni, M. B., & Bhaiyya, M. (2025). Artificial intelligence and machine learning for colorimetric detections: Techniques, applications, and future prospects. In *Trends in Environmental Analytical Chemistry* (Vol. 48). Elsevier B.V. https://doi.org/10.1016/j.teac.2025.e00280

Tabassum, F., Azim, M. I., Islam, M. R., Rahman, M. A., Ali, L., Rahman, M. M., & Hossain, M. J. (2025). Energy data security and pricing model in local energy markets using artificial intelligence. *Applied Energy, 401*, Article 126737. https://doi.org/10.1016/j.apenergy.2025.126737

Tian, J., & Zhang, Y. (2025). Does artificial intelligence help in improving human capital based educational development? Evidence from 29 countries. *Technology in Society, 83*. https://doi.org/10.1016/j.techsoc.2025.103004

Viola, L., Mohammadi, S., Dotta, D., Hesamzadeh, M. R., Baldick, R., & Flynn, D. (2024). Ancillary services in power system transition toward a 100% non-fossil future: Market design challenges in the United States and Europe. *Electric Power Systems Research, 236*, Article 110885. https://doi.org/10.1016/j.epsr.2024.110885

Yue Yim, I. H. (2024). A critical review of teaching and learning artificial intelligence (AI) literacy: Developing an intelligence-based AI literacy framework for primary school education. In *Computers and Education: Artificial Intelligence* (Vol. 7). Elsevier B.V. https://doi.org/10.1016/j.caeai.2024.100319

Zhao, X., Ye, Y., Han, Y., & Huo, B. (2025). Impact of informality on operational security in emerging markets. *International Journal of Production Economics, Article 109716*. https://doi.org/10.1016/j.ijpe.2025.109716