

Critical factors affecting digital resilience in the Sri Lankan banking sector: a systematic review

Harini Jayasundara* and A.P.R. Wickramarachchi

Department of Industrial Management, University of Kelaniya, Kelaniya, Sri Lanka

*Corresponding author: harinigithma@gmail.com

 <https://orcid.org/0009-0006-8072-1036>

Received: 29.10.2024

Revised: 13.11.2024

Accepted: 09.12.2024

Online: 15.12.2024

Abstract Digitalizing the Sri Lankan banking sector has heightened its vulnerability to cyber threats and operational disruptions, making digital resilience critical for maintaining continuity. This systematic literature review (SLR) employs the Technology-Organization-Environment (TOE) framework to explore and categorize the factors affecting digital resilience in the Sri Lankan Banking Sector. A review of 45 studies from 2016 to 2024 highlights three major categories: technological factors (e.g., cybersecurity measures, IT infrastructure, and emerging technologies like AI and blockchain), organizational factors (e.g., leadership, employee training, and strategic planning), and environmental factors (e.g., regulatory compliance, customer trust, and vendor management). The findings suggest that a holistic and integrated approach is necessary for enhancing digital resilience, specifically balancing technological innovation, organizational agility, and compliance with regulatory requirements. Moreover, the review identifies significant gaps in the current literature regarding Sri Lanka-specific empirical studies, recommending future research into the application of emerging technologies such as AI and blockchain to enhance resilience in developing economies. Additionally, the study proposes strategies to improve digital resilience, including strengthening cybersecurity infrastructure, fostering leadership-driven digital initiatives, updating business continuity plans, and advocating for flexible regulatory frameworks that balance innovation with security. The study underscores the need for an integrated approach to digital resilience. It suggests that future research should focus on targeted interventions to enhance resilience within the Sri Lankan banking sector and broader financial domain.

Keywords: Banking sector, Cybersecurity, Digital resilience, Sri Lanka

Introduction

The global banking sector is under increasing pressure to advance digital infrastructure and adopt emerging technologies to meet evolving market demands and enhance operational efficiency. This shift towards digital banking has led to greater reliance on online platforms, exposing banks to heightened risks of cyber threats and system vulnerabilities (Dupin et al., 2022). The frequency and sophistication of cyberattacks such as ransomware, phishing, and Distributed Denial-of-Service (DDoS) attacks, have increased globally, targeting financial institutions due to their critical role in managing assets and ensuring economic stability (Hobbs and Gennarini, 2021). For Sri Lanka's banking sector, which is pivotal in supporting economic growth, the move to digital platforms has introduced additional challenges, including cyberattacks, data breaches, and system failures. These vulnerabilities underscore the

urgent need for robust digital resilience strategies to safeguard operational continuity, ensure regulatory compliance, and maintain customer trust (Klimontowicz, 2016; Weerasinghe, 2023).

Digital resilience, defined as the capacity of an organization's information systems to withstand and recover from digital disruptions, goes beyond traditional IT resilience. It includes using information systems proactively to prevent, adjust to, respond to, and recover from technology-based disruptions. It ensures digital systems withstand disruptions while maintaining continuous operations and safeguarding data integrity (Boh et al., 2023; Kohn, 2023). Integrating financial technologies (fintech), such as mobile banking, blockchain, and digital wallets, has amplified cybersecurity risks globally (Kaur et al., 2021). These fintech applications often introduce vulnerabilities, requiring enhanced security



measures. For instance, vulnerabilities in mobile payment systems or blockchain networks, result in security breaches or fraud when exploited (Schatz et al., 2017). Insufficient regulatory frameworks and technological limitations further exacerbate these risks, leaving financial institutions increasingly vulnerable to sophisticated and evolving cyber threats (Baur-Yazbeck et al., 2019). Sri Lanka's banks must navigate these challenges while aligning technological advancements with organizational readiness and regulatory frameworks to ensure services remain secure, dependable, and responsive in an increasingly digitized environment (Manzini et al., 2022; Resano, 2023).

Despite the importance of digital resilience, empirical studies specifically focused on the financial sector remain limited. While a reasonable amount of literature exists on digital resilience across various domains, such as healthcare, education, and supply chain management, a significant gap remains in those that address the unique challenges of the financial sector (Hassan et al., 2024). Financial institutions face the burden of safeguarding sensitive customer data and ensuring uninterrupted services. Yet, many existing studies focus on isolated factors, such as cybersecurity or regulatory compliance, without examining interdependencies. This siloed approach risks overlooking the dynamic interactions between technological, organizational, and environmental dimensions (Hobbs & Gennarini, 2021; Dupin et al., 2022). For instance, a strong cybersecurity system may fail without organizational support or alignment with environmental pressures, such as regulatory requirements (Schatz et al., 2017).

The need for such an understanding is even more pronounced in Sri Lanka, where little to no empirical research has examined how different factors collectively impact the ability of banks to withstand and recover from digital disruptions. The country's banking sector faces unique vulnerabilities, including underdeveloped technological infrastructure, varying levels of digital literacy, and stringent regulatory requirements imposed by the Central Bank of Sri Lanka (CBSL). These issues are compounded by limited resources to implement advanced resilience strategies effectively (Alodhiani, 2023).

While global financial institutions are increasingly investing in technologies like

Artificial Intelligence (AI) and advanced analytics to predict and mitigate cyber threats, Sri Lankan banks often lack the economic and technical resources to adopt such measures at scale (Mohamed & Ali, 2020; Oyeniyi et al., 2024). The ability of banks to address these challenges and harness technological advancements to strengthen resilience is critical to the success of the Digital Sri Lanka 2030 strategy (Weerasinghe, 2023). Therefore, addressing these gaps is essential not only for the operational integrity of financial institutions but also for ensuring economic stability during times of disruption.

This systematic literature review (SLR) addresses these challenges using the Technology-Organization-Environment (TOE) framework introduced by Tornatzky et al. (1990). Traditionally applied to evaluate technology adoption, the TOE framework is adapted in this study to identify and analyze the critical factors influencing digital resilience. By categorizing these factors into technological, organizational, and environmental dimensions, the TOE framework provides a structured approach to understanding how they interact to shape resilience in a sector increasingly reliant on digital infrastructure.

Accordingly, this review aims to answer the research question: *What critical factors significantly influence digital resilience in the Sri Lankan banking sector?* The study also seeks to achieve the objective of identifying and analyzing the factors influencing digital resilience in the Sri Lankan banking sector using the TOE framework.

As Sri Lanka implements its Digital Sri Lanka 2030 strategy, understanding these factors is essential for enhancing the sector's ability to withstand rapid technological advancements and evolving cyber threats (Weerasinghe, 2023). This study contributes to the growing body of knowledge by examining how the TOE framework can be applied to digital resilience, offering actionable insights for policymakers, practitioners, and academics. The findings from this review will provide a conceptual framework that integrates technological, organizational, and environmental factors, advancing the understanding of how banks can respond to digital disruptions. This will guide the development of strategic recommendations that strengthen digital resilience in Sri Lanka's banking sector and ensure the stability and security of financial services.

Methodology

In conducting this SLR on the factors affecting digital resilience in the banking sector, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) 2020 guidelines were rigorously followed to ensure a transparent and replicable review process (Page et al., 2021). This approach enabled systematic identification, screening, and inclusion of studies relevant to the research objectives.

Review Question

The review question that guided the literature search in this study was: What are the critical factors influencing digital resilience in the banking sector?

Eligibility Criteria

The eligibility criteria were selected to ensure the inclusion of relevant and high-quality studies focusing on contemporary insights into digital resilience in the banking sector. The selection criteria and corresponding rationale are outlined in Table 1.

Table 1: Article Selection Criteria

Criterion	Inclusion	Exclusion	Rationale
Publication Type	Peer-reviewed journal articles, conference papers, Scopus-indexed book chapters, and reputable white papers.	Grey literature, blogs, and non-peer-reviewed sources.	Ensures the inclusion of credible and impactful research by focusing on rigorously reviewed and validated sources.
Publication Period	From 2016 to 2024, with a focus on studies published after 2019.	Studies published before 2016.	Captures significant advancements in digital resilience strategies, especially post-pandemic shifts.
Language(s)	English	Non-English publications	Maintains consistency in analysis and avoids potential mistranslations or misinterpretations.
Publication Scope	Studies focused on digital resilience in banking, including cyber-resilience and IT resilience, with theoretical, empirical, or practical perspectives.	Studies focusing on unrelated sectors or with limited methodological rigor.	Ensures a comprehensive analysis of multiple factors influencing resilience in the banking sector.
Data Availability	Studies with full-text availability.	Abstracts only or studies with missing full-text access.	Avoids reliance on incomplete or speculative information.

Information Sources

The literature search was conducted using a comprehensive approach across multiple key platforms. The primary search was initiated through Google Scholar, which linked relevant studies across major academic databases, including ScienceDirect, IEEE Xplore Digital Library, SpringerLink, Wiley Online Library, and Emerald

Insight. These databases were selected for their extensive coverage of peer-reviewed literature pertinent to digital resilience in the banking sector. The search period, from April to September 2024, focused on capturing the most recent and relevant studies.

Both published and grey literature were considered, the latter specifically targeting white papers and reports from reputable institutions.

Mendeley was utilized for reference management and to remove duplicates, ensuring accuracy and replicability in the search process.

Search Strategy

The search strategy employed a combination of structured search strings and natural language queries to capture a comprehensive range of relevant studies. The primary search string used was: ("Banking industry" AND ("Digital Resilience" OR "Cyber resilience" OR "IT resilience")).

Including "Sri Lankan banking sector" in the primary search string did not yield specific results. However, relevant studies on the topic were identified when the phrase "Sri Lankan banking sector" was used independently.

SciSpace was utilized to complement traditional search methods by providing AI-driven literature recommendations. Queries such as "*What are the technological factors affecting digital resilience?*" provided AI-synthesized answers referencing existing studies. These cited references were manually cross-verified for accuracy and relevance before being considered for inclusion in the review. The incorporation of AI in this manner streamlined the literature search, uncovering studies that might have been overlooked in traditional database searches.

Selection Process

The article selection process employed a combination of AI-assisted tools and manual review to ensure the inclusion of relevant literature. Initial screening was conducted using AI tools SciSpace and Gemini, facilitating the rapid identification and exclusion of non-relevant studies. These tools were used to assess whether

the identified studies contained relevant information on the study's focus area. Queries were carefully crafted to avoid bias, with the tools primarily clustering studies based on keywords and extracting relevant passages for consideration. These excerpts were not taken at face value but underwent thorough manual cross-checking to ensure their accuracy and alignment with the review's objectives.

Following the AI-assisted screening, a detailed manual review was performed to verify the thematic alignment and contribution of each study to the research objectives.

The selection process was documented in a PRISMA flow diagram, illustrating each stage from identification to the final inclusion of studies.

Data Items

The data items for this SLR were defined to align with the study's objectives, focusing on identifying key factors influencing digital resilience within the banking sector. These factors were broadly categorized into technological, organizational, and environmental domains. These categories were systematically populated with associated studies, and the findings were tabulated to facilitate a structured and comprehensive analysis.

Results and Discussion

Study Selection

The literature search identified 597 records, of which 45 studies were included in the SLR after rigorous screening and selection. The detailed selection process, including the number of records at each stage, is illustrated in the PRISMA flow diagram (Figure 1).

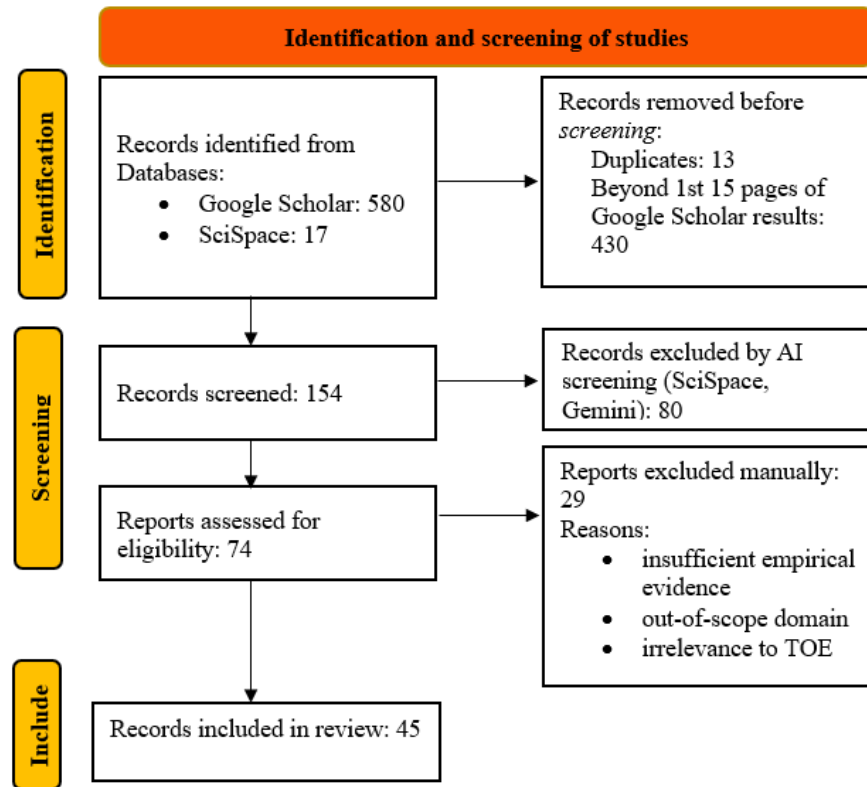


Figure 1. PRISMA flow diagram for article selection.

Thematic Categorization of Findings

The studies revealed a range of factors influencing digital resilience, which were categorized into three key groups: technological, operational, and environmental, based on the TOE framework. This categorization provides a structured approach to understanding the complex nature of digital resilience within the Sri Lankan banking sector.

Notably, no significant factors were identified outside these groups, reinforcing the comprehensiveness of the TOE framework. The following sections offer a detailed examination of each category's contributions to digital resilience, critically analyzing the literature to highlight key insights for enhancing resilience strategies in the banking sector.

Technological Factors

Technological factors play an integral role in shaping digital resilience. Among them, cybersecurity is a critical factor, driven by the escalating complexity of cyber threats. Both

Christine and Thinyane (2020) and Ewuga et al. (2024) emphasize the growing complexity of cyberattacks, which necessitates continuous advancements in cybersecurity strategies. Christine and Thinyane (2020) further suggest the broader societal impact of adverse cyber events. Ewuga et al. (2024) focus specifically on the banking sector, underscoring the need to safeguard sensitive financial information against such threats.

Khan and Malaika (2021) add another layer by linking fintech developments with increased cybersecurity risks, suggesting that innovations such as mobile banking and digital wallets may expose additional vulnerabilities when IT infrastructure is inadequately protected. This view complements the proactive stance of Manzini et al. (2022) and Hassan et al. (2024) who advocate for the establishment of Security Operations Centers (SOCs) and regular security assessments to enhance resilience.

For Sri Lankan banks, the urgency for robust cybersecurity audits and enhanced network management is heightened due to the country's unique vulnerabilities, as noted by Jayamaha

(2016), who highlights the challenges posed by limited technological resources, primarily at the government level. Additionally, advancements in cybersecurity often require complementary organizational measures, such as leadership-driven initiatives and employee training, to be effective (Dawodu et al., 2023). The consensus across these studies underscores the necessity of continuously improving cybersecurity measures to strengthen resilience. Yet, Sri Lanka's banking sector faces distinct infrastructural challenges that make achieving these improvements more complex.

Beyond cybersecurity, the stability of core IT infrastructure is equally essential for safeguarding digital resilience. Dupin et al. (2022) and Cavallini et al. (2023) both emphasize that a resilient IT infrastructure minimizes the risk of operational disruptions, contributing to overall system stability. This is complemented by Roy (2022), who notes the growing reliance on IT infrastructure, particularly in areas with unstable power and internet connectivity, such as rural regions in Sri Lanka, and how such dependencies introduce additional risks. Khan and Malaika (2021) add to this discussion by emphasizing the need for developed backup systems and disaster recovery plans to ensure continuity in case of infrastructural failures. This perspective is especially relevant for Sri Lankan banks, where maintaining infrastructure stability is paramount in the face of frequent power outages and unreliable internet services. The consistent message across these studies is that without robust core infrastructure, the banking sector remains vulnerable to disruptions that could significantly undermine its digital resilience.

Emerging technologies, such as cloud computing, Artificial Intelligence (AI), machine learning (ML), and blockchain, are increasingly recognized for their potential to enhance digital resilience. Cloud computing, for instance, offers scalability and redundancy, which are critical for maintaining operations during disruptions. Mehedintu and Soava (2022) and Vanderbist (2020) argue that cloud migration provides banks with scalability and redundancy, enabling them to maintain operations during disruptions. However, Resano (2023) raises concerns about the over-reliance on cloud service providers, which can introduce systemic risks if not responsibly managed. This risk is further discussed by Manzini et al. (2022) who note that while cloud computing

offers scalability and reduces operational risks for central banks, it also shifts some control away from the organization, potentially increasing dependence on third-party providers. Adopting cloud computing could help Sri Lankan banks address operational risks by reducing dependence on physical infrastructure. However, its successful implementation depends heavily on robust vendor management practices and adherence to regulatory frameworks, suggesting the intersection of technological, organizational, and environmental considerations.

The role of AI and ML in digital resilience is becoming increasingly significant in the areas of risk assessment and fraud detection. Studies by Dawodu et al. (2023) and Vanderbist (2020) argue that AI technologies enhance risk management by allowing banks to anticipate better and mitigate cybersecurity threats. Similarly, Ndukwe and Baridam (2023) and Farayola (2024) highlight AI's role in proactive fraud detection, where its ability to analyze large volumes of data in real-time enables early identification of potential threats. However, Khan and Malaika (2021) caution that while AI holds great promise, its mitigation and prevention capabilities are still in their early stages, suggesting a need for further innovation and development.

Blockchain technology is increasingly seen as an emerging technology affecting digital resilience in the banking sector. Studies by Mishra et al. (2023) and He (2021) emphasize blockchain's ability to enhance security and transparency, reducing the risk of fraud and unauthorized access through its immutable ledger system. Farayola (2024) and Bhattacharya and Bhattacharjee (2022) extend this discussion by highlighting blockchain's potential to transform financial transactions, offering a decentralized transaction-based system that enhances operational security and transparency. For Sri Lankan banks, integrating blockchain into their digital systems could enhance their resilience to cyber-attacks and fraud. However, Ewuga et al. (2024) cautioned against the challenges of aligning blockchain with existing security frameworks. Integrating blockchain technology presents significant challenges, as the transition from centralized to decentralized systems requires new approaches to risk management.

Emerging technological advancements in cybersecurity, IT infrastructure, and technologies

such as Artificial Intelligence (AI), Machine Learning (ML), and blockchain interact dynamically with organizational and environmental factors to shape digital resilience. For instance, cybersecurity measures depend not only on technical innovations but also on organizational leadership and employee training to implement and sustain these solutions effectively (Dawodu et al., 2023). Similarly, cloud computing's ability to provide redundancy and scalability requires robust vendor management practices and regulatory compliance, bridging the technological, organizational, and environmental dimensions (Manzini et al., 2022). Blockchain adoption, while enhancing operational security, is shaped by external regulatory frameworks and organizational strategies to manage its integration challenges effectively (Mishra et al., 2023; Ewuga et al., 2024). These interdependencies underscore the need for a coordinated approach, where technological advancements are supported by aligned organizational strategies and external regulatory environments.

Accordingly, the studies reviewed demonstrate a broad consensus on the importance of continuous technological advancement in ensuring digital resilience. While cybersecurity, infrastructure stability, and the adoption of emerging technologies such as cloud computing, AI, and blockchain all contribute significantly, each comes with its own set of risks and challenges that require ongoing innovation and careful management. For Sri Lankan banks, these insights present the need for a balanced approach that combines local infrastructure with innovative technologies to enhance overall digital resilience.

Organizational Factors

Leadership and organizational culture are pivotal in driving digital resilience within the banking sector. Juliana et al. (2023) argue that leadership-driven digital initiatives enable organizations to effectively monitor situations, communicate information, obtain resources, and adapt to changing circumstances. This perspective aligns with Al-Alawi and Al-Bassam (2020), who stress the importance of board-level leadership in embedding resilience within corporate strategy, arguing that a proactive IT strategy at the executive

level ensures resilience is a core organizational objective rather than a reactive measure.

In comparison, Trenerrey et al. (2021) emphasize that leadership supporting innovation, combined with a culture of continuous learning, plays a fundamental role in fostering resilience through digital transformation. Safitra et al. (2023) further validate this by noting that a culture of accountability and innovation enables cyber resilience, suggesting that leadership's role extends beyond oversight to actively nurturing an environment conducive to resilience. Together, these sources reinforce the idea that digital resilience is deeply rooted in an organizational culture led by forward-thinking leadership, where both strategic foresight and a commitment to adaptability are the keys to long-term success.

Employee awareness and training are equally essential, as human error remains a primary vulnerability. Both Dawodu et al. (2023) and Koli and Saini (2023) highlight the effectiveness of structured training programs in reducing risks associated with human error, particularly against social engineering attacks, often the weakest cybersecurity link. Godbole et al. (2021) argue that while advanced cybersecurity systems are critical, they must be supported by a security-conscious culture in which employees actively participate as the organization's "human firewall" against external threats. Echoing this, Al-Alawi and Al-Bassam (2020) underscore the importance of continuous awareness programs to instill a proactive security culture. This focus on employee awareness becomes particularly relevant for Sri Lankan banks, where Bandara et al. (2019) point out that digital literacy levels vary, especially among older employees. Tailored training programs to enhance technical competence and mitigate risks from human error are thus essential in the Sri Lankan context, ensuring that all staff are equipped to handle technological risks effectively.

Strategic planning is also fundamental to digital resilience. Jayalath and Premarathne (2021) discuss the role of strategic planning as the backbone of successful digital transformation, highlighting the importance of a comprehensive digital strategy that aligns with overall business objectives. They emphasize that resilience requires not only a sound digital strategy but also the integration of digital processes across departments to support core operations. This strategic alignment is critical in

the banking sector, where resilience directly impacts service continuity and client trust. Complementing this view, Roy (2022) highlights the importance of impact analysis and hazard assessments as prerequisites for developing robust disaster recovery and continuity plans, underscoring that banks remain vulnerable to operational disruptions without such planning.

The significance of Business Continuity Planning (BCP) and risk management within strategic planning is reinforced by Galaitsi et al. (2023) who highlight BCP as a crucial framework to ensure continuity of essential activities during crises. Regular reviews of BCP are essential to ensure adaptability to evolving threats. Godbole et al. (2021) extend this perspective, advocating for the integration of Cyber Crisis Management Plans (CCMP) to address the unique risks posed by cyber incidents. They suggest that CCMP allows for a rapid response to cyber crises, minimizing downtime and mitigating financial and reputational risks. Additionally, Dawodu et al. (2023) and Koli and Saini (2023) highlight the importance of proactive risk management strategies, such as threat modeling and vulnerability assessments, to identify and address potential risks before they manifest into major disruptions.

The organizational factors discussed above dynamically interact with technological and environmental dimensions. For example, leadership-driven strategies directly influence the adoption and effective use of technologies like AI and blockchain, ensuring alignment with organizational goals and regulatory frameworks (Juliana et al., 2023; Mishra et al., 2023). Similarly, employee training programs enhance the operationalization of advanced technologies while fostering a security-conscious culture that complements external compliance requirements (Dawodu et al., 2023; Resano, 2023). Strategic planning also bridges organizational and environmental factors by aligning internal risk management practices with regulatory demands and stakeholder expectations (Galaitsi et al., 2023). These interactions suggest the necessity of developing cohesive strategies that integrate organizational agility with technological advancements and evolving regulations within the Sri Lankan banking sector.

Together, these insights emphasize that organizational factors, including leadership,

culture, employee training, and strategic planning, form the foundation of a bank's digital resilience. Effective resilience strategies depend on adaptive leadership, a proactive organizational culture, comprehensive employee awareness, and meticulously planned continuity frameworks. For Sri Lankan banks, where infrastructural and resource challenges present unique obstacles, embedding these organizational factors at all levels is essential to sustaining resilience in an increasingly digital banking environment.

Environmental Factors

Environmental factors, especially regulatory frameworks and third-party vendor management play an essential role in shaping digital resilience within the banking sector. Regulatory factors are critical for ensuring data protection and operational continuity, as highlighted by Dawodu et al. (2023) and Ewuga et al. (2024) who discuss how compliance with frameworks like the General Data Protection Regulation (GDPR), revised Payment Services Directive (PSD2), and Basel III is necessary for resilience in a globally regulated environment. These frameworks establish stringent data security and operational stability standards, serving as foundational benchmarks for resilience in financial institutions.

Similarly, Godbole et al. (2021) mentions the importance of adhering to standards such as ISO 27001 for information security management, those set by the National Institute of Standards and Technology (NIST), and the Capability Maturity Model for CERT Resilience Management Model (CERT-RMM). Although these standards do not exclusively target resilience, their comprehensive cybersecurity requirements strengthen resilience by promoting robust security practices. Additionally, Hassan et al. (2024) offer insights from Nigeria, where the Central Bank's Risk-Based Cybersecurity Framework and Open Banking Framework illustrate how regulatory bodies can foster innovation without compromising security and compliance.

In Sri Lanka, the cybersecurity regulations and digital banking initiatives set by the Central Bank of Sri Lanka (CBSL) create a dual-focus regulatory environment that seeks to balance security imperatives with the promotion of innovation. However, Jayamaha (2016) pointed out the

challenge for Sri Lankan banks in balancing stringent regulatory compliance with the need for technological innovation. This is echoed by Manzini et al. (2022) who call for agile regulatory frameworks that adapt to emerging risks. This need for flexibility in regulatory supervision acknowledges that rigid compliance structures may stifle technological advancement, hindering resilience.

Beyond regulatory compliance, customer confidence and trust are critical environmental factors affecting digital resilience. Hassan et al. (2024) argue that, particularly in emerging markets with youthful and tech-savvy demographics, maintaining customer trust is fundamental for digital service adoption. This perspective aligns with Shah (2016) and Maragaoda (2019) who emphasize that customers' confidence in online banking directly influences their willingness to use digital platforms. In contrast, Sahu et al. (2024) warn that frequent cybersecurity incidents, such as phishing and data breaches, erode customer trust and discourage the adoption of digital banking, suggesting that resilience efforts must not only be operational but also address public perceptions of security.

Third-party vendors and outsourced services significantly impact digital resilience, as their management introduces potential vulnerabilities beyond banks' immediate control. Khan and Malaika (2021) and Cooper (2024) discuss the growing reliance on third-party providers, such as cloud service providers, cybersecurity firms, and payment gateway vendors, which introduces vendor risks. For Sri Lankan banks, managing these risks is essential as dependence on external services can expose them to vulnerabilities beyond their immediate control. Effective vendor management practices, including regular audits, collaborative risk assessments, and strict Service Level Agreements (SLA), can help mitigate these risks (Khan & Malaika, 2021; Cooper, 2024). Bandara et al. (2019) also highlighted the significance of diversifying suppliers and establishing robust supplier management protocols to reduce exposure to single-point failures and increase operational flexibility.

Environmental factors do not function in isolation; they interact dynamically with both technological and organizational dimensions to shape digital resilience. In Sri Lanka, the CBSL plays a significant role in regulating the banking sector and mandating strict cybersecurity protocols, data protection standards, and risk management practices. These regulations influence the technologies banks can adopt, emphasizing cybersecurity systems to ensure compliance while fostering organizational practices that integrate these systems effectively (Manzini et al., 2022 and Hassan et al., 2024). Additionally, CBSL regulations necessitate active involvement from leadership to meet compliance requirements, ensuring digital resilience remains a strategic priority for financial institutions. Maintaining customer trust often involves leveraging technologies like blockchain for transparency and requiring organizations to develop communication strategies that reinforce public confidence (Shah, 2016; Mishra et al., 2023). Vendor management practices also illustrate this interdependence, as technological systems for monitoring third-party risks must align with organizational policies and CBSL requirements (Cooper, 2024).

Accordingly, environmental factors, including regulatory compliance, customer trust, and vendor management, collectively shape digital resilience within the banking sector. While regulatory frameworks and standards establish a secure operational foundation, banks must balance these requirements with technological innovation to remain competitive. Furthermore, public-facing aspects such as customer trust underscore the need for secure, transparent operations that meet stakeholder expectations. For Sri Lankan banks, effectively navigating the complex interplay of stringent regulations, evolving customer demands, and third-party relationships is essential to fostering a resilient and adaptive digital environment in an interconnected global financial ecosystem.

Table 2 summarizes the key factors influencing digital resilience in the Sri Lankan banking sector, categorized into technological, organizational, and environmental domains, along with supporting literature.

Table 2: Key factors affecting digital resilience and supporting literature.

Category	Factor	Supporting Literature
Technological Factors	Cybersecurity Infrastructure	(Christine & Thinyane, 2020; Ewuga et al., 2024; Hassan et al., 2024; Jayamaha, 2016; Khan & Malaika, 2021; Manzini et al., 2022)
	Core location IT Infrastructure	(Cavallini et al., 2023; Dupin et al., 2023; Khan & Malaika, 2021; Roy, 2022)
	Cloud Computing	(Manzini et al., 2022; Resano, 2023; Mehedintu & Soava, 2022; Vanderbist, 2020)
	AI and ML	(Dawodu et al., 2023; Khan & Malaika, 2021; Ndukwe and Baridam, 2023; Farayola, 2024; Vanderbist, 2020)
	Blockchain Technology	(Bhattacharya and Bhattacharjee, 2022; Ewuga, 2024; He, 2021; Mishra et al., 2023; Farayola, 2024)
Organizational Factors	Leadership and Organizational Culture	(Juliana et al., 2023; Al-Alawi & Al-Bassam, 2020; Trencher et al., 2021; Safitra et al., 2023)
	Employee Awareness and Training	(Dawodu et al., 2023; Koli and Saini, 2023; Godbole et al., 2021; Bandara et al., 2019)
	Strategic Planning	(Jayalath & Premarathne, 2021; Roy, 2022; Galaitsi et al., 2023; Godbole et al., 2021; Dawodu et al., 2023; Koli and Saini, 2023)
	Regulatory Compliance	(Ewuga et al., 2024; Dawodu et al., 2023; Godbole et al., 2021; Hassan et al., 2024; Jayamaha, 2016; Manzini et al., 2022, Joseph, 2021)
Environmental Factors	Customer Confidence and Trust	(Hassan et al., 2024; Shah, 2016; Maragaoda, 2019; Sahu et al., 2024)
	Vendor and Third-party Risk Management	(Khan & Malaika, 2021; Cooper, 2024; Manzini et al., 2022)

Application of the TOE Framework

The Technology-Organization-Environment (TOE) framework, developed by Tornatzky et al. (1990), provides a structured lens for categorizing and analyzing technological innovation within organizations. Traditionally applied to technology adoption, the framework is adapted in this study to represent the factors affecting digital resilience in the Sri Lankan banking sector. Accordingly, this study organizes the identified factors into three dimensions: technological, organizational, and environmental, providing valuable insights into the key components influencing digital resilience and their interconnectedness.

In the context of Sri Lankan banks, factors such as cybersecurity infrastructure, cloud computing, and AI/ML adoption, directly align with the technology dimension of the TOE framework. These factors represent the technological readiness and innovations necessary to address growing cyber threats and maintain operational continuity. Ewuga et al. (2024) and Khan and Malaika (2021)

underscore the critical role of leveraging these technologies to enhance digital resilience, specifically when integrated with complementary organizational and environmental practices.

The organizational dimension of the TOE framework is equally relevant. The literature emphasizes the importance of leadership, strategic planning, and employee training, which form the backbone of organizational resilience. Juliana et al. (2023) and Al-Alawi and Al-Bassam (2020) underscore the need for leadership to align digital initiatives with organizational objectives, fostering a culture that supports innovation and adaptability. This is particularly critical for Sri Lankan banks, where varying digital literacy levels necessitate targeted training programs to mitigate human error (Bandara et al., 2019).

The environmental dimension focuses on external pressures, including regulatory compliance and customer trust, which play a fundamental role in shaping resilience. In Sri Lanka, the regulatory landscape is governed by the Central Bank of Sri Lanka (CBSL) and international standards such as

ISO 27001, ensuring cybersecurity and operational stability (Joseph, 2021). As emphasized by Hassan et al. (2024) and Ewuga et al. (2024) compliance with these standards not only ensures security but also builds customer trust, a vital component of resilience in a digital-first world. As part of this environmental influence, vendor management also demands stringent practices to minimize third-party risks, further emphasizing the interconnectedness of technological, organizational, and environmental factors in fostering resilience.

While the TOE framework categorizes factors, this study expands on its application by illustrating how these dimensions interconnect dynamically within the context of digital resilience. Technological advancements, such as AI and blockchain, often necessitate organizational readiness, including leadership-driven strategies and employee training, for successful implementation. Similarly, regulatory frameworks drive both technological adoption and organizational alignment, ensuring compliance and fostering customer trust. Vendor management exemplifies this interconnectedness, requiring technological tools for monitoring risks and organizational policies for oversight, aligned with external regulatory standards (Khan & Malaika, 2021; Mishra et al., 2023).

This expanded representation signifies the bidirectional relationships among all three components. For example, technological factors such as cybersecurity are shaped by both organizational strategies (e.g., leadership engagement) and environmental pressures (e.g., CBSL regulations). Likewise, customer trust, an environmental factor, is influenced by technological transparency (e.g., blockchain) and organizational communication strategies (Shah, 2016; Mishra et al., 2023).

Figure 2 depicts this adapted framework, integrating the identified factors within the technological, organizational, and environmental

dimensions of the TOE framework while emphasizing their interrelationships. The framework incorporates bidirectional arrows to represent the dynamic interactions among these dimensions and includes labeled pathways from the factors to digital resilience to indicate their distinct impacts.

Applying the TOE framework to digital resilience allows Sri Lankan banks to develop a structured, comprehensive approach that integrates technology, internal organizational capabilities, and external regulatory pressures. This approach addresses gaps in the current literature, offering a dynamic and adaptable model for resilience that aligns with both global best practices and local challenges. The application of the TOE framework thus provides a meaningful basis for understanding and improving resilience strategies in the banking sector, where regulatory compliance, organizational agility, and technological innovation are all critical to mitigating disruptions and maintaining operational continuity.

Strategies to Enhance Digital Resilience

Several key strategies should be adopted to improve digital resilience in the Sri Lankan banking sector, addressing the identified technological, organizational, and environmental factors. A fundamental starting point is to strengthen cybersecurity infrastructure. With increasing cyber threats targeting financial institutions, Sri Lankan banks must invest in cybersecurity audits and developing Security Operations Centers (SOCs) to ensure continuous threat monitoring and fast incident response. These measures are crucial given the sector's unique infrastructural challenges and limited resources. Moreover, adopting zero-trust architectures and AI-driven threat detection systems would further enhance the bank's proactive defenses against sophisticated attacks.

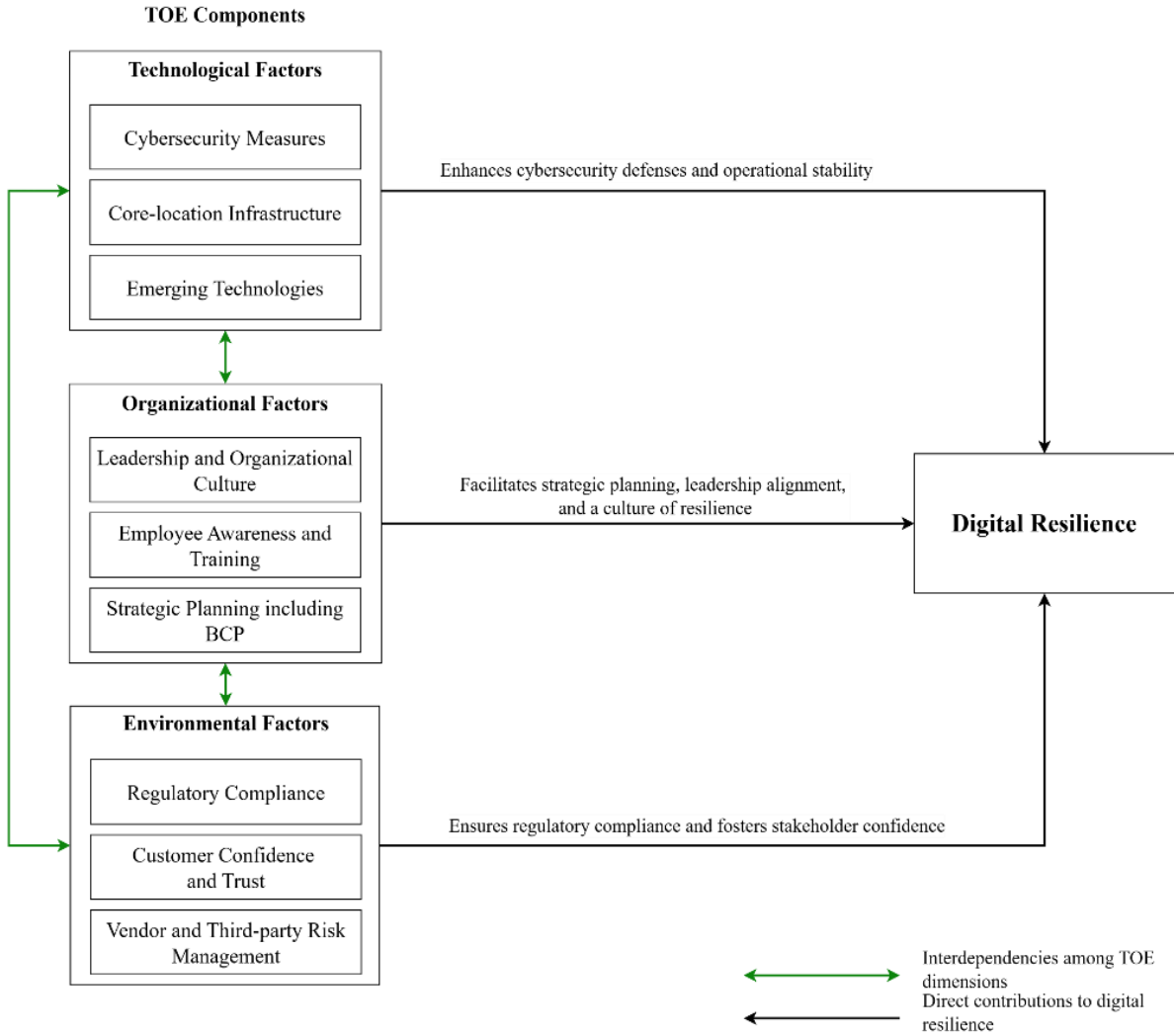


Figure 2. Adapted TOE framework illustrating interconnected factors affecting digital resilience in the Sri Lankan banking sector.

Adopting cloud computing presents opportunities to mitigate local infrastructure limitations by offering scalability and operational flexibility. However, this reliance on third-party vendors introduces external risks. Therefore, banks must develop comprehensive vendor management strategies, such as diversifying service providers and instituting stringent Service Level Agreements (SLAs), to ensure reliability and minimize vendor-related vulnerabilities. Regular vendor risk assessments should be conducted to mitigate potential disruptions that could arise from third-party failures or cyberattacks targeting outsourced services.

From an organizational perspective, leadership plays a pivotal role in fostering a culture that

prioritizes digital resilience. Bank leadership should embed resilience into long-term corporate strategies, ensuring alignment between digital initiatives and organizational goals. Employee training programs tailored to varying levels of digital literacy should be prioritized to minimize human error, which remains a significant cybersecurity vulnerability. Sri Lankan banks, where staff digital competency can be uneven, should invest in continuous cybersecurity training to empower employees to function as the first line of defense against social engineering and other cyber threats. Such efforts will cultivate a security-conscious culture within the organization.

Business Continuity Planning (BCP) and Cyber Crisis Management Plans (CCMP) should be updated regularly to address potential operational

disruptions. These plans must incorporate threat modeling, impact analyses, and emerging cyber risks to ensure they are relevant in a fast-evolving digital landscape. Moreover, Sri Lankan banks should implement disaster recovery (DR) plans that go beyond traditional recovery methods, emphasizing cyber resilience to manage both physical and digital disruptions. This will ensure continuity of critical banking services during unforeseen crises, such as cyberattacks or natural disasters, which could otherwise cripple the sector's operations.

On the environmental front, regulatory compliance and customer trust are central to maintaining resilience. Adhering to Central Bank regulations and global standards, such as ISO 27001, is essential for securing customer data and ensuring operational stability. However, balancing compliance with innovation remains a challenge for Sri Lankan banks. Banks should actively engage with regulatory bodies to advocate for agile regulatory frameworks that accommodate technological advancements while maintaining stringent security requirements. This would enable the banking sector to remain compliant without stifling innovation, especially with the rise in fintech solutions and blockchain technology.

Fostering customer trust in digital platforms is critical for broader digital banking adoption. To achieve this, banks should prioritize transparent communication regarding their data protection practices and continuously update their fraud detection systems. Technologies such as blockchain can be leveraged to provide secure and transparent transactions, further instilling confidence in digital banking services. In parallel, banks must invest in educational campaigns that enhance public understanding of cybersecurity measures, reinforcing customer trust in the safety and reliability of their digital interactions with financial institutions.

Conclusion and Recommendations

This systematic literature review identifies the key factors influencing digital resilience in the Sri Lankan banking sector, emphasizing the importance of an integrated approach framed by the Technology-Organization-Environment (TOE) framework. Technological advancements, such as cybersecurity infrastructure and cloud computing,

coupled with strategic leadership and regulatory compliance, are critical to sustaining operational continuity and mitigating digital disruptions. The interconnectedness of these factors highlights the need for a coordinated approach, integrating technological innovation, organizational agility, and regulatory frameworks.

The review contributes to understanding digital resilience by highlighting the interconnectedness of these factors and their collective impact. It argues that addressing these factors in isolation is insufficient; instead, a coordinated approach involving technological innovation, human capital development, and regulatory alignment is essential for achieving and maintaining digital resilience. This integrated perspective is critically relevant for Sri Lankan banks, where challenges such as limited infrastructure, varying levels of digital literacy, and stringent regulatory demands complicate efforts to build resilience.

Despite its contributions, this review acknowledges several limitations. Chief among them is the scarcity of Sri Lanka-specific literature, which necessitated the extrapolation of findings from broader regional or global studies. While these extrapolations provide valuable insights, they may not fully capture the unique dynamics of the Sri Lankan banking sector, particularly concerning local infrastructure and regulatory nuances. To address this, future research must prioritize empirical studies conducted within Sri Lanka, allowing for more accurate contextualization of findings and the formulation of tailored recommendations.

Another limitation is the reliance on secondary data and literature-based insights. While this approach is methodologically robust for identifying trends and gaps, it does not account for real-time challenges or sector-specific nuances that can only be captured through primary data collection. Future studies should therefore incorporate interviews, surveys, and case studies involving Sri Lankan banking professionals to provide deeper insights into the practical implementation of digital resilience strategies.

Further research should delve deeper into the roles of emerging technologies such as AI, ML, and blockchain in enhancing digital resilience. These technologies hold significant promise for improving risk assessment, fraud detection, and operational scalability. However, their feasibility

and scalability in the Sri Lankan banking context, given its regulatory and infrastructural constraints, warrant closer examination. Similarly, cross-border regulatory frameworks and their implications for Sri Lankan banks present a critical area for exploration. As the financial sector becomes increasingly interconnected, understanding how global standards such as GDPR influence local compliance requirements will provide valuable insights for maintaining resilience in a globalized environment.

The interconnected nature of the banking sector with fintech firms, third-party vendors, and regional markets also requires focused attention. These relationships create both opportunities and vulnerabilities, necessitating a comprehensive understanding of how vendor risks and compliance requirements can be managed effectively. Future research could identify best practices for ensuring alignment between vendor relationships, technological innovation, and regulatory compliance, all of which are vital for fostering digital resilience in a globally networked financial system.

The TOE framework's relevance to analyzing digital resilience has been presented by this review, but its application in the Sri Lankan banking context remains underexplored. Empirical research should investigate how the identified factors interact in practice, confirming the framework's applicability and effectiveness in addressing the unique challenges faced by Sri Lankan banks. Additionally, understanding customer trust in digital banking services is critical for resilience. Research could examine how public perceptions of cybersecurity incidents, awareness campaigns, and digital literacy levels influence customer confidence and their willingness to adopt digital banking services in Sri Lanka.

Lastly, given the rapid evolution of cyber threats and financial technologies, dynamic risk management models that integrate technological, organizational, and environmental factors are necessary. These models would allow banks to proactively address emerging challenges, such as new forms of cyberattacks or regulatory shifts, by fostering adaptability and innovation. Developing such models would provide a more holistic and forward-looking approach to resilience, enabling Sri Lankan banks to mitigate disruptions

effectively while maintaining operational continuity.

Future efforts should focus on deepening local insights, fostering global adaptability, and developing integrative frameworks that align with both local realities and global best practices.

Acknowledgements

The authors gratefully acknowledge the contributions of previous researchers whose work informed and shaped the foundation of this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Author Contributions

Harini Jayasundara- Conceptualization, Methodology, Formal analysis, Resource collection, Writing original draft, review and editing.

A.P.R. Wickramarachchi: Supervision, Validation, Writing – review and editing.

References

- Al-Alawi, A. I., & Al-Bassam, S. (2020). Study of the cybercrime cost and the risk of criminal threats to the banking sector. *JOURNAL OF XI AN UNIVERSITY OF ARCHITECTURE & TECHNOLOGY*, XII(III). <https://doi.org/10.37896/jxat12.04/770>
- Alodhiani, A. A. B. (2023). Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review. *Arab Journal for Humanities and Social Sciences*, 20. <https://doi.org/10.59735/arabjhs.vi20.55>
- Bandara, O., Vidanagamachchi, K., & Wickramarachchi, R. (2019). *A Model for Assessing Maturity of Industry 4.0 in the Banking Sector*. Proceedings of the International Conference on Industrial Engineering and Operations Management. https://www.researchgate.net/publication/335421711_A_Model_for_Assessing_Maturity_of_Industry_40_in_the_Banking_Sector
- Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). *CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT: Challenges and*

- potential solutions for financial inclusion. CGAP. <https://documents1.worldbank.org/curated/en/209721593689624542/pdf/Cyber-Security-in-Financial-Sector-Development--and-Potential-Solutions-for-Financial-Inclusion.pdf>
- Bhattacharya, A., & Bhattacharjee, S. (2022). A REVIEW ON APPLICATIONS OF BLOCKCHAIN IN BANKING SECTORS. *International Journal of Engineering Applied Sciences and Technology*, 7(4), 156–159. <https://doi.org/10.33564/ijeast.2021.v06i03.005>
- Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2023). Building Digital Resilience Against Major Shocks. *MIS Quarterly*, 47(1), 343–360. https://www.researchgate.net/publication/368469691_Building_Digital_Resilience_Against_Major_Shocks
- Cavallini, S., Soldi, R., Casalini, G., Verdi, G., & Grasso, A. (2023). Digital Resilience. In *European Committee of the Nations*. European Union. <https://doi.org/10.2863/5099>
- Christine, D. I., & Thinyane, M. (2020). Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries. *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCOM/CyberSciTech)*, 71–78. <https://doi.org/10.1109/dasc-pico-m-cbdcom-cybercitech49142.2020.00027>
- Cooper, M. (2024). *Building Resilient Supply Chains: Perspectives on Procurement Risk Management*. <https://doi.org/10.20944/preprints202407.0609.v1>
- Dawodu, N. S. O., Omotosho, N. A., Akindote, N. O. J., Adegbite, N. a. O., & Ewuga, N. S. K. (2023). CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES. *Computer Science & IT Research Journal*, 4(3), 220–243. <https://doi.org/10.51594/csitrj.v4i3.659>
- Dupin, J., Pascal, A., & Godé, C. (2022, September 6). A Systematic Literature Review on Digital Resilience in Organizations: Towards a Conceptualization. <https://shs.hal.science/halshs-03959505>
- Ewuga, N. S. K., Egieya, N. Z. E., Omotosho, N. A., & Adegbite, N. a. O. (2024). ISO 27001 IN BANKING: AN EVALUATION OF ITS IMPLEMENTATION AND EFFECTIVENESS IN ENHANCING INFORMATION SECURITY. *Finance & Accounting Research Journal*, 5(12), 405–425. <https://doi.org/10.51594/farj.v5i12.684>
- Farayola, N. O. A. (2024). REVOLUTIONIZING BANKING SECURITY: INTEGRATING ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, AND BUSINESS INTELLIGENCE FOR ENHANCED CYBERSECURITY. *Finance & Accounting Research Journal*, 6(4), 501–514. <https://doi.org/10.51594/farj.v6i4.990>
- Galaitsi, S. E., Pinigina, E., Keisler, J. M., Pescaroli, G., Keenan, J. M., & Linkov, I. (2023). Business continuity Management, operational resilience, and organizational resilience: commonalities, distinctions, and synthesis. *International Journal of Disaster Risk Science*, 14(5), 713–721. <https://doi.org/10.1007/s13753-023-00494-x>
- Godbole, T., Gochhait, S., & Ghosh, D. (2021). Developing a framework to measure cyber resilience behaviour of Indian bank employees. In *Smart innovation, systems and technologies* (pp. 299–309). https://doi.org/10.1007/978-981-16-4177-0_31
- Hassan, N. a. O., Ewuga, N. S. K., Abdul, N. a. A. A. A., Abrahams, N. T. O., Oladeinde, N. M., & Dawodu, N. S. O. (2024). CYBERSECURITY IN BANKING: A GLOBAL PERSPECTIVE WITH a FOCUS ON NIGERIAN PRACTICES. *Computer Science & IT Research Journal*, 5(1), 41–59. <https://doi.org/10.51594/csitrj.v5i1.701>
- He, Q. (2021). Application of blockchain technology in commercial banks. *E3S Web of Conferences*, 235, 03070. <https://doi.org/10.1051/e3sconf/202123503070>
- Hobbs, B., & Gennarini, A. (2021, October 12). *Why digital resilience must be a top priority for banks*. EY. <https://www.ey.com/eng/banking-capital-markets-risk-regulatory-transformation/why-digital-resilience-must-be-a-top-priority-for-banks>
- Jayalath, J. a. R. C., & Premaratne, S. C. (2021). Analysis of Digital Transformation challenges to overcome by Banks and Financial

- Institutions in Sri Lanka. *International Journal of Research Publications*, 84(1). <https://doi.org/10.47119/ijrp100841920212260>
- Jayamaha, R. (2016). THRIVING IN A DIGITAL WORLD: NON-BANKS HAVE CHALLENGED RETAIL BUSINESS OF BANKS. In *Apbsrilanka*. Association of Professional Bankers Sri Lanka. <https://apbsrilanka.com/2016-convention-articles/>
- Joseph, R. (2021, July 29). Sri Lanka Banking Report. KPMG. <https://kpmg.com/lk/en/home/insights/2021/06/sri-lanka-banking-report-june-2021.html>
- Juliana, B. M., Prabowo, H., Alamsjah, F., & Hamsal, M. (2023). Building Organizational Resilience by developing Customers Orientation, Digital Adoption and Organizational Agility: An Empirical Study in The Indonesian Banking Industry. *Quality - Access to Success*, 24(197). <https://doi.org/10.47750/qas/24.197.09>
- Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding Cybersecurity management in FinTech. In *Future of business and finance*. <https://doi.org/10.1007/978-3-030-79915-1>
- Khan, A., & Malaika, M. (2021). Central bank risk management, fintech, and cybersecurity. *IMF Working Paper*, 2021(105), 1. <https://doi.org/10.5089/9781513582344.001>
- Klimontowicz, M. (2016). Knowledge as a Foundation of Resilience on Polish Banking Market. *Electronic Journal of Knowledge Management*, 14(1), 58–72. https://www.researchgate.net/publication/299388870_Knowledge_as_a_Foundation_of_Resilience_on_Polish_Banking_Market
- Kohn, V. (2023). *Operationalizing digital resilience—A systematic literature review on opportunities and challenges*. Proceedings of the 56th Hawaii International Conference on System Sciences. <https://hdl.handle.net/10125/103412>
- Koli, J. M., & Saini, A. K. (2023). Assessing Information Security Governance in public sector Banks of India. *International Journal of Engineering Technology and Management Sciences*, 7(5), 103–116. <https://doi.org/10.46647/ijetms.2023.v07i05.012>
- Manzini, D., Oosthuizen, R., & Chikwanda, H. K. (2022). A Resilience Framework for Digital Transformation in the Banking sector: A Systems Thinking approach. *2022 IEEE 28th International Conference on Engineering, Technology and Innovation (ICE/ITMC) & 31st International Association for Management of Technology (IAMOT) Joint Conference*. <https://doi.org/10.1109/ice/itmc-iamot55089.2022.10033305>
- Maragaoda, W. S. K. (2019). *Customers' motivation to embrace digital banking in Sri Lanka; A case study of Sampath Bank PLC*. <https://www.researchbank.ac.nz/server/api/core/bitstreams/75343e14-db42-420e-a3d5-acc7da9cab8/content>
- Mehedintu, A., & Soava, G. (2022). A structural framework for assessing the digital resilience of enterprises in the context of the technological revolution 4.0. *Electronics*, 11(15), 2439. <https://doi.org/10.3390/electronics11152439>
- Mishra, R., Singh, R. K., Kumar, S., Mangla, S. K., & Kumar, V. (2023). Critical success factors of Blockchain technology adoption for sustainable and resilient operations in the banking industry during an uncertain business environment. *Electronic Commerce Research*. <https://doi.org/10.1007/s10660-023-09707-3>
- Mohamed, H., & Ali, H. (2020). Finding solutions to cybersecurity challenges in the digital economy. In *Advances in finance, accounting, and economics book series* (pp. 80–96). <https://doi.org/10.4018/978-1-7998-4390-0.ch005>
- Ndukwe, E. R., & Baridam, B. (2023). A Graphical and qualitative review of literature on AI-based Cyber-Threat intelligence (CTI) in banking sector. *European Journal of Engineering and Technology Research*, 8(5), 59–69. <https://doi.org/10.24018/ejeng.2023.8.5.3103>
- Oyeniya, N. L. D., Ugochukwu, N. C. E., & Mhlongo, N. N. Z. (2024). DEVELOPING CYBERSECURITY FRAMEWORKS FOR FINANCIAL INSTITUTIONS: A COMPREHENSIVE REVIEW AND BEST PRACTICES. *Computer Science & IT Research Journal*, 5(4), 903–925. <https://doi.org/10.51594/csitrj.v5i4.1049>

- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. <https://doi.org/10.1136/bmj.n71>
- Resano, J. R. M. (2023). Digital resilience and financial stability. The quest for policy tools in the financial sector. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4336381>
- Roy, A. (2022). Analysis of business continuity plan in banking sector. *International Journal for Research in Applied Science and Engineering Technology*, 10(8), 982–987. <https://doi.org/10.22214/ijraset.2022.46326>
- Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, 15(18), 13369. <https://doi.org/10.3390/su151813369>
- Sahu, A., Khemka, M., Agrwal, A., Sahu, B., & Shadan, M. (2024). Consumer Confidence in Digital Finance: Trust Dynamics in Online Banking. *International Journal for Multidisciplinary Research*, 6(3). <https://doi.org/10.36948/ijfmr.2024.v06i03.19946>
- Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, 12(2), 53. <https://doi.org/10.15394/jdfsl.2017.1476>
- Shah, K. K. (2016). Electronic Banking: Its use and challenge in Nepal. *Academic Voices a Multidisciplinary Journal*, 5, 9–15. <https://doi.org/10.3126/av.v5i0.15845>
- Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation*. Free Press.
- Trenerry, B., Chng, S., Wang, Y., Suhaila, Z. S., Lim, S. S., Lu, H. Y., & Oh, P. H. (2021). Preparing Workplaces for Digital Transformation: An Integrative Review and Framework of Multi-Level Factors. *Frontiers in Psychology*, 12. <https://doi.org/10.3389/fpsyg.2021.620766>
- Vanderbist, D. (2020). *Digital Resilience: Managing Cyber-Security and Data Privacy*. www.researchgate.net/publication/344308920_Digital_Resilience_Managing_Cyber-Security_and_Data_Privacy
- Weerasinghe, N. (2023, November 3). *Achieving Resilience through Digitalization, Sustainability and Sectoral Transformation*. Forum on Sri Lanka's Sustainable Development Trajectories and Pathways, Sri Lanka. www.cbsl.gov.lk/en/node/15407