Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 8, 2025

AN OPTIMIZED FRAMEWORK OF CYBERSECURITY TECHNIQUES FOR PROTECTING THE PERSONAL INFORMATION OF ACCOUNT HOLDERS IN INTERNET BANKING SYSTEM OF PAKISTAN

Yasir Ali Solangi[*1], Abdullah Maitlo[2], Mumtaz Hussain Mahar[3], Zulfiqar Ali Solangi[4]

[*1,2] *Department of Computer Science, Shah Abdul Latif University Khairpur*
[3] *Department of Computer Science, SZABIST University, Larkana Campus*
[4] *Jubail Technical Institute, Education Sector Royal Commission Jubail, SA*

[*1]yasir_solangi@yahoo.com,[2]abdullah.maitlo@salu.edu.pk,[3]mumtaz.mahar@lrk.szabist.edu.pk,
[4]solangi_z@rcjy.edu.sa

DOI: https://doi.org/10.5281/zenodo.16779280

Keywords
Cybersecurity, Cyber Defense Framework, Information Security

Article History
Received: 27 April, 2025
Accepted: 20 July, 2025
Published: 08 August, 2025

Corresponding Author: *
Yasir Ali Solangi

Abstract
The rapid innovation in digital technology has revolutionized banking services, enabling automatic financial transactions and transforming customer engagement through Internet banking. This shift has led to reduced operational costs and enhanced customer satisfaction; however, it has also introduced serious vulnerabilities, especially in countries like Pakistan where Internet banking remains a relatively new but growing phenomenon. Fraudsters now exploit sophisticated online techniques, raising the stakes for banks facing internal, external, and regulatory cybersecurity threats. This study employed a quantitative methodology using structured survey responses from 350 account holders across Pakistan to examine these challenges. Through descriptive statistics, reliability testing, and Reliability Analysis, Cronbach's Alpha, the research validated a four-layer Cyber Defense Framework designed to protect digital financial information. Findings revealed significant gaps in technological awareness, procedural security, and trust in digital transactions, underscoring the urgent need for robust frameworks. Practically, the framework provides actionable insights for financial institutions and regulators supporting more resilient system designs, adaptive cybersecurity strategies, and enhanced legal mechanisms to safeguard users. By aligning technological innovation with strategic security measures, this study contributes a context-sensitive blueprint for strengthening Pakistan's banking sector against emerging digital threats.

INTRODUCTION

The proliferation of the Internet as a marketing and communication tool represents a significant challenge for the banking sector. Current scholarly research indicates that the Internet continues to generate business prospects, with numerous organizations investing in this digital platform to conduct their marketing operations. This widespread adoption has enabled e-commerce to provide enhanced services and convenience to customers. Consequently, the banking industry has incorporated Internet banking for both financial operations and information dissemination regarding products and services (JANAHI, 2016).

Online banking has fundamentally transformed traditional financial institutions (Sathye, 1999). This banking evolution has been facilitated through the digitization and automation of activities for operational efficiency (Bradley & Stewart, 2003). The Internet and web offer potential competitive advantages for banks primarily in cost reduction and meeting consumer demands (Chandio, 2011). This modern online banking system presents both opportunities and potential negative implications stemming from technological unfamiliarity, potentially increasing customer financial risks and damaging bank reputations. In Pakistan, Internet banking remains a relatively recent development expected to expand with increased computer and Internet service penetration, robust legal frameworks, alleviation of online transaction security concerns, and improved communication reliability (Electronic Banking in Pakistan, 2018). The increasing use of the Internet and global online networks has created new commercial opportunities and trading relationships while simultaneously providing sophisticated avenues for fraudulent activities. Governmental authorities have responded with more stringent cyber legislation, often through international collaboration to establish common transparency and accountability standards globally (Lavion, 2018). The prevalence of companies with limited awareness of their fraud exposure remains concerning. This year's Global Economic Crime and Fraud Survey, comprising insights from over 7,200 participants across 123 territories, endeavors to expose fraud issues and illuminate critical strategic challenges confronting organizations. In developing nations such as Pakistan, banking fraud has evolved into a fundamental business concern, primarily due to the expanded magnitude and influence of fraudulent activities in our digital environment. Indeed, it could almost be considered a significant industry in its own right (Lavion, 2018). Pakistani banking institutions currently navigate a continuous stream of cyber security challenges—whether internal, external, or regulatory. The current climate necessitates an innovative, more comprehensive view of security threats, one that acknowledges the genuine nature of the risk not merely as operational overhead but as a shadow industry capable of permeating every domain, sector, and function. The obscured nature of these threats makes inadequate awareness within the banking sector particularly hazardous. The pertinent question is not whether your institution experiences fraud, but rather your cognizance of how this threat impacts your organization and clientele. A proactive, fully informed approach to combating these issues is essential (Bradley & Stewart, 2003, Lavion, 2018). Consequently, this research will assess both evident cyber security threats facing Pakistan's banking sector and identify the perceptual limitations preventing a comprehensive understanding of the situation.

Literature Review

The contemporary advancements in mobile and cloud computing, electronic commerce, and social applications are fundamentally altering business perspectives globally. Organizations are formulating strategies to harness the unexplored advantages of these technological innovations for information exchange and internet-based commercial activities (Broadhurst & Chang, 2013). In this Information Technology era, novel developments are impacting all aspects of society. Various organizations, including the banking sector, are integrating IT solutions to enhance productivity and expand their clientele. Banks worldwide are increasingly implementing Internet Banking services. The necessity for Electronic Banking emerged in South Asia approximately 5-7 years ago, establishing itself as a crucial component for effective banking management. The financial industry recognized this shift promptly, with Pakistani banks transitioning from traditional ledger systems to computerized operations. Despite foreign banks introducing this concept to South Asia, they have yet to implement advanced Internet Banking services in Pakistan (Electronic Banking in Pakistan, 2018). Information technology serves financial services by enhancing operational efficiency, improving customer service, mitigating risks, and supporting strategic decisions. Pakistan's government has instructed the State Bank to permit internet merchant accounts for electronic fund transfers, redesign foreign trade processes, accept electronic orders, establish e-commerce divisions in financial institutions, and facilitate electronic clearing and reporting across all banks (Pakistan, 2018).

Approximately eighty percent of total business transactions occur online, necessitating robust

security measures to minimize transaction failures and customer dissatisfaction. Cyber Security extends beyond protecting an organization's local IT infrastructure to encompass broader network and technological frameworks (Gartenstein-Ross & Dabruzzi, 2007). The significance of cyber security is paramount in the development and implementation of critical computing and communication infrastructure (Hecht, 2007).

Cybersecurity in Internet Banking

The rapid digitization of financial services has made internet banking a cornerstone of modern banking systems. However, this transformation has also exposed account holders to a range of cyber threats including identity theft, phishing, malware attacks, and unauthorized access(Jameaba & Ssenyonga Jameaba, 2022). Cybersecurity in banking refers to the technologies and practices designed to safeguard digital assets, customer data, and transactional integrity(Adejumo & Ogburie, 2025). Recent research and industry guidelines emphasize a range of best practices to safeguard personal information in online banking environments. Key measures include multi-factor authentication (MFA), which strengthens identity verification through multiple credentials beyond traditional passwords, and end-to-end encryption(Ahmed & Jafri, 2024), which ensures that sensitive data remains confidential during transmission. Biometric authentication methods such as fingerprint and facial recognition offer secure, user-friendly access(Morake, 2021). The use of official banking apps equipped with encryption and sandboxing further fortifies the mobile banking experience(Khang, 2025). Real-time transaction monitoring aids in the early detection of suspicious activity, while proactive user education and phishing awareness campaigns empower customers to identify and avoid common scams(Gadimov & Birihanu, 2025). Together, these strategies create a robust framework for digital banking security.

Cybersecurity Landscape in Pakistan

Pakistan's National Cyber Security Policy 2021 sets forth comprehensive objectives for safeguarding digital infrastructure, with a particular focus on financial systems(Saleem et al., 2024). Complementing this, the State Bank of Pakistan (SBP) has introduced formal regulations for internet banking security, prioritizing risk mitigation, authentication protocols, monitoring systems, and user awareness(Ahmed & Jafri, 2024). However, practical challenges persist most notably in regulatory enforcement, technological adoption, and public confidence in digital platforms. The optimized framework developed in this study responds to these gaps through a layered, context-aware approach tailored to the Pakistani banking environment. Notably, existing literature, though rich in global models, offers limited insights for developing economies like Pakistan. Key omissions include locally adapted cybersecurity strategies, consideration of user behavior and cultural context, and mechanisms for real-time accountability in digital banking(Ahmed & Jafri, 2024). This research advances the discourse by addressing those limitations and offering a framework built on empirical validation and regional relevance**Proposed**

Research Framework and Global Cybersecurity Frameworks

Globally acknowledged cybersecurity frameworks including NIST CSF, ISO/IEC 27001, and CIS Controls offer systematic methodologies for safeguarding digital systems(Luis Salas-Riega et al., 2025). They highlight key security dimensions such as preventive measures e.g., encryption, access control, and secure configurations), detective capabilities like system monitoring, anomaly identification, and audit logging, responsive protocols focused on incident handling and recovery, and governance mechanisms that ensure compliance, transparency, and continuous advancement. The four-layer framework proposed in this research study effectively encapsulates these core principles, presenting a streamlined and contextually adapted model specifically designed for the digital banking landscape in Pakistan.

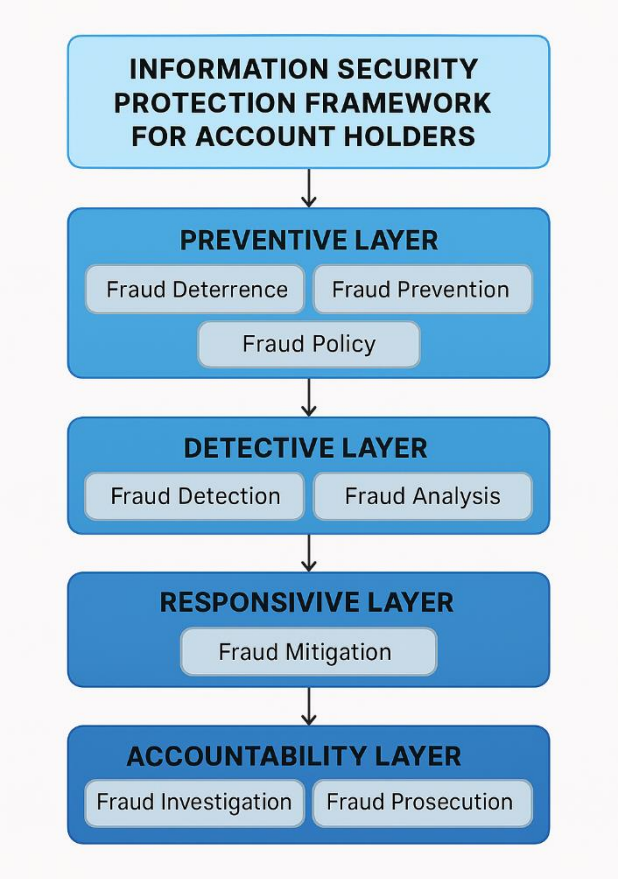

Figure 1 Proposed Research Framework

Table 1

Studies on Cybersecurity in Digital Banking	Findings
Cybersecurity Threats in Digital Banking: A Comprehensive Analysis	- Explores phishing, ransomware, and DDoS attacks in banking - Proposes multi-layered defense strategies including zero trust architecture and threat intelligence sharing - Highlights a 91% increase in credential harvesting attempts in financial institutions
Cybersecurity in Banking and Financial Services: Protecting Digital Assets	- Focuses on identity theft, fraud prevention, and future cybersecurity trends - Emphasizes the role of encryption, authentication, and secure development practices
Cybersecurity Risks in Online Banking: A Detailed Review and Preventive Strategies	- Evaluates recent cyber incidents and their financial impact - Recommends AI, Big Data analytics, and continuous risk assessment for resilience

Studies on Cybersecurity in Digital Banking	Findings
An Integrated Cybersecurity Risk Management Framework for Online Banking Systems	- Proposes a threat-based risk model tailored for banking environments - Assesses vulnerabilities and mitigation strategies with real-world applicability
A Survey of Cybersecurity Laws, Regulations, and Policies in Technologically Advanced Nations: A Case Study of Pakistan	- Compares Pakistan's cybersecurity posture with countries like the US, India, and Singapore - Highlights gaps in governance, institutional coordination, and policy implementation
Implementation Strategies of Cybersecurity in Pakistan	- Analyzes the National Cyber Security Policy 2021 - Identifies weaknesses in legislative enforcement and institutional readiness
Pakistan's Cyber Security Governance: Challenges and Way Forward	- Discusses governance issues, lack of strategic oversight, and the need for a National Cyber Security Authority - Offers recommendations for improving institutional synergy and policy execution

In Table 1 these studies collectively reinforce the relevance and strength of the proposed framework by affirming the necessity of a multi-layered cybersecurity approach, mirroring the proposed four-layer model. They underscore the importance of adapting international best practices to align with Pakistan's specific regulatory and technological context. Moreover, they expose critical shortcomings in existing frameworks particularly in responsiveness and accountability that proposed optimized solution is designed to address. The literature underscores the critical need for a multi-layered cybersecurity approach in internet banking. The proposed framework comprising **Preventive, Detective, Responsive, and Accountability layers** is well-supported by global best practices and national policy directives. It offers a promising solution to enhance the protection of personal information for account holders in Pakistan's digital banking landscape.

Methodology

This study involved the whole population of banks in Pakistan. As of 30 January 2025, there is a total of 7 public banks, and 11 private banks in Pakistan that consist of 10 local and 8 foreign banks as recorded in the data obtained from State Bank of Pakistan website at https://www.sbp.org.pk/psd/2015/c3-annexure-a.pdf#. This study employed a quantitative descriptive research design to evaluate the efficacy and perception of a four-layer cybersecurity framework. Preventive, Detective, Responsive, and Accountability in safeguarding the personal information of bank account holders using internet banking in Pakistan. Data were collected through a structured survey questionnaire administered to a purposefully selected sample of seven internet banking users, representing both public and private sector banks(Moser & Korstjens, 2018). The questionnaire comprised Likert-scale items designed to measure participants' awareness, trust, and experience across the four framework layers. This study employed a quantitative descriptive research design to evaluate the efficacy and perception of a four-layer cybersecurity framework. Preventive, Detective, Responsive, and Accountability in safeguarding the personal information of bank account holders using internet banking in Pakistan. A total of 700 structured survey questionnaires were distributed among internet banking users in both public and private sector banks, selected through purposive sampling. Of these, 350 completed responses were received, yielding a response rate of 50%.

The questionnaire incorporated Likert-scale measurements designed to evaluate users' cognizance, confidence, and interaction throughout the four dimensions of the framework (Akter et al., 2013). The survey instrument was formulated according to the suggested investigative structure and additional scholarly works concerning digital protection and protected online financial platforms. Survey

components encompassed multiple categories: Section A gathered participant background information including chronological age, professional history, sex categorization, professional role, etc. Section B aimed to measure participants' understanding of digital safety risks and overall knowledge about protective measures, while Section C examined banking technological foundation, offerings, data architecture, and other pertinent topics. Analytical procedures employed fundamental statistical calculations (arithmetic average, distribution counts, variance measures) to comprehend patterns and user perspectives, alongside internal consistency verification utilizing Cronbach's alpha coefficient to confirm measurement reliability. Contrastive methodologies were implemented to investigate perceptual variations between consumers of state-owned and independent banking networks. All principles of research ethics including informed consent, privacy protection, and responsible information management were strictly adhered to throughout the investigation process (Jamieson, 2004).

Data Analysis and Results

i. **Demographics**

A total of 350 responses were analyzed for the study, representing a diverse sample from Pakistan's banking sector in Table 2. Of these, 217 respondents (62%) were affiliated with public sector banks, while the remaining 133 respondents (38%) belonged to private sector banks. This near-even distribution offers a balanced perspective, enabling comparative insights between public and private banking institutions.

ii. **Table 3 Descriptive Statistics per Construct**

Construct	Mean	Standard Deviation (SD)	Dominant Response
Fraud Deterrence (FD)	3.92	0.73	Agree
Fraud Prevention (FP)	4.05	0.68	Agree
Fraud Detection (FD)	4.02	0.72	Agree
Fraud Mitigation (FM)	3.88	0.79	Agree
Fraud Analysis (FA)	4.10	0.64	Agree
Fraud Policy (FP)	4.00	0.70	Agree
Fraud Investigation (FI)	3.85	0.75	Agree
Fraud Prosecution (FPR)	3.80	0.78	Neither agree nor disagree to Agree

Based on the descriptive statistics in Table 3, respondents showed a generally positive perception across all fraud-related constructs measured in the study. The highest mean score was observed for Fraud Analysis (M = 4.10, SD = 0.64), indicating strong agreement and perceived importance of analytical measures in combating fraud. This was closely followed by Fraud Prevention (M = 4.05, SD = 0.68) and Fraud Detection (M = 4.02, SD = 0.72), suggesting respondents value proactive and reactive mechanisms almost equally. Fraud Policy (M = 4.00, SD = 0.70) also received strong endorsement, reflecting the significance of formalized guidelines. Meanwhile, constructs like Fraud Deterrence, Fraud Mitigation, and Fraud Investigation scored slightly lower but still maintained agreement levels, with mean scores ranging from 3.85 to 3.92. Fraud Prosecution had the lowest mean score (M = 3.80, SD = 0.78), indicating more neutral views, spanning from "neither agree nor disagree" to "agree." Overall, these findings highlight widespread consensus among respondents in favor of strategic fraud management elements, with emphasis on analysis, prevention, and detection.

iii. Table 4 **Reliability Analysis – Cronbach's Alpha**

Construct	Cronbach's Alpha
Fraud Deterrence	0.82
Fraud Prevention	0.85
Fraud Detection	0.84
Fraud Mitigation	0.81

Construct	Cronbach's Alpha
Fraud Analysis	0.86
Fraud Policy	0.83
Fraud Investigation	0.80
Fraud Prosecution	0.79

The reliability analysis using Cronbach's Alpha in Table 4 revealed strong internal consistency across all measured constructs in the study. Fraud Analysis demonstrated the highest reliability with an alpha of 0.86, signifying a high degree of agreement among items within that scale. Fraud Prevention (α = 0.85) and Fraud Detection (α = 0.84) also showed excellent reliability, underscoring the robustness of these constructs in the context of cybersecurity practices. Constructs such as Fraud Policy (α = 0.83), Fraud Deterrence (α = 0.82), and Fraud Mitigation (α = 0.81) maintained solid reliability, confirming their relevance and coherence within the framework. Fraud Investigation and Fraud Prosecution yielded slightly lower but still acceptable alpha values of 0.80 and 0.79, respectively, indicating consistent measurement. Overall, the analysis confirms the soundness of the instrument used, with all constructs exceeding the commonly accepted threshold of 0.70 for reliability in social science research.

Discussion

Recent studies have emphasized the growing need for robust cybersecurity frameworks tailored to the financial sector. For instance, a study conducted a comprehensive review of cybersecurity practices across financial institutions and concluded that existing frameworks(Adejumo & Ogburie, 2025) while foundational are increasingly inadequate against evolving threats. Their study advocated for adaptable, technology-driven models that integrate regulatory agility and stakeholder collaboration(Paul et al., 2023). Compared to current study findings, which show strong user confidence in fraud analysis (Mean = 4.10, Cronbach's α = 0.86), the proposed framework demonstrates higher perceived effectiveness in analytical and policy-driven layers than those reported in previous studies reference above. Similarly, the research study proposed an integrated cybersecurity risk management framework for online banking systems, emphasizing threat modeling and contextual risk assessment(Azura et al., 2025). Their evaluation highlighted gaps in real-time responsiveness and user trust. The findings of data analysis, however, show relatively strong scores in fraud mitigation (Mean = 3.88, α = 0.81) and fraud detection (Mean = 4.02, α = 0.84), suggesting that Pakistani account holders perceive their banks as more responsive and technologically equipped than the global average reported in the recent studies. In another study, cybersecurity risks in Indian and South African banking were evaluated, revealing moderate user confidence in fraud prosecution and investigation mechanisms(Afzal et al., 2024; Akinbowale et al., 2024). The research findings align with this trend, showing lower scores in fraud prosecution (Mean = 3.80, α = 0.79), indicating that legal follow-up and victim compensation remain areas of concern across developing economies. Overall, the proposed optimized framework not only aligns with global best practices but also addresses localized gaps in responsiveness and accountability. The comparative strength in fraud analysis and policy perception among Pakistani users suggests that banks are making strides in strategic cybersecurity planning, though legal enforcement and prosecution mechanisms require further development.

Conclusion

This study offers a localized, empirically validated cybersecurity framework tailored to the specific challenges of internet banking in Pakistan. By addressing fraud detection, mitigation, policy formation, and prosecution layers, the framework enhances technological resilience and deepens user trust. The data highlights strong user confidence in analytical layers, particularly fraud analysis (Mean = 4.10, α = 0.86) and detection (Mean = 4.02, α = 0.84), suggesting that Pakistani banks have made notable strides in countering digital threats. However, moderate scores in fraud prosecution (Mean = 3.80, α = 0.79) indicate persistent gaps in legal redress and victim support issues common across emerging economies for further institutional and legal

reinforcement to improve enforcement and accountability(Rusydi, 2024). This research introduces a context-sensitive, empirically supported cybersecurity framework designed to safeguard personal information within Pakistan's internet banking system. The four-layer model encompassing fraud deterrence, prevention, detection, mitigation, analysis, policy, investigation, and prosecution captures a comprehensive approach aligned with both global standards and localized challenges (Asaju, 2024; Pham & Nguyen, 2023).

Practical Implications and Future work

The findings of this study hold valuable practical implications for stakeholders in Pakistan's financial sector. Banks can use the proposed framework to fortify digital security operations, improve incident responsiveness, and enhance customer confidence, while regulators may draw from its layered design to strengthen national cybersecurity policies and legal enforcement mechanisms. Technology developers can also apply these insights to create adaptive banking platforms embedded with proactive fraud management tools. Looking forward, future research should explore longitudinal assessments of framework effectiveness over time, incorporate AI-driven fraud prediction models, and investigate the influence of user behavior and digital literacy on cybersecurity outcomes. Expanding the framework through cross-country comparisons and deeper integration of behavioral dimensions will further enhance its robustness and global relevance.

REFERENCES:

Adejumo, A. P., & Ogburie, C. P. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, *25*(3), 1527–1541.

Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., & Shoeb, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: an integrated model approach. *Journal of Financial Services Marketing*, *29*(4), 1503–1523.

Ahmed, F., & Jafri, S. W. A. (2024). A critical assessment of the State Bank of Pakistan's vision 2020 in shaping the financial landscape: Prospects and realities. In *Governance and Policy Transformations in Central Banking* (pp. 169–195). IGI Global Scientific Publishing.

Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, *10*(1).

Akter, S., D'Ambra, J., & Ray, P. (2013). Development and validation of an instrument to measure user perceived service quality of mHealth. *Information & Management*, *50*(4), 181–195.

Asaju, B. J. (2024). Standardization and regulation of V2X cybersecurity: analyzing the current landscape, identifying gaps, and proposing frameworks for harmonization. *Advances in Deep Learning Techniques*, *4*(1), 33–52.

Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology*, 1–20.

Bradley, L., & Stewart, K. (2003). A Delphi study of Internet banking. *Marketing Intelligence & Planning*, *21*(5), 272–281.

Broadhurst, R., & Chang, L. Y. C. (2013). Cybercrime in Asia: trends and challenges. In *Handbook of Asian criminology* (pp. 49–63). Springer.

Chandio, F. H. (2011). *Studying acceptance of online banking information system: A structural equation model*. Brunel University Brunel Business School PhD Theses.

Electronic Banking in Pakistan. (2018). [Essays, UK. (November 2018).]. https://www.ukessays.com/essays/banking/electronic-banking.php?vref=1

Gadimov, E., & Birihanu, E. (2025). Real-time suspicious detection framework for financial data streams. *International Journal of Information Technology*, 1–17.

Gartenstein-Ross, D., & Dabruzzi, K. (2007). The convergence of crime and terror. *Policing Terrorism Report*, *1*.

Hecht, J. (2007). When web browsers turn bad. *New Scientist*, *194*(2602), 28–29.

Jameaba, M., & Ssenyonga Jameaba, M. (2022). *Digitalization, emerging technologies, and financial stability: Challenges and opportunities for the banking industry*.

Jamieson, S. (2004). *Likert scales : how to (ab) use them*. 1217–1218. https://doi.org/10.1111/j.1365-2929.2004.02012.x

JANAHI, Y. (2016). *University of Bradford eThesis Overcoming Barriers to Adoption Through the Use of Biometrics Submitted for the Degree of*. University of Bradford.

Khang, A. (2025). *Shaping cutting-edge technologies and applications for digital banking and financial services*. Productivity Press.

Lavion, D. (2018). *Pulling fraud out of the shadows*.

Luis Salas-Riega, J., Riega-Virú, Y., Ninaquispe-Soto, M., & Miguel Salas-Riega, J. (2025). Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats. *International Journal of Advanced Computer Science & Applications*, *16*(6).

Morake, T. A. (2021). *A multi-factor authentication approach for e-banking*. University of Johannesburg (South Africa).

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9–18.

Pakistan, S. B. of. (2018). *REGULATIONS FOR THE SECURITY OF INTERNET BANKING PAYMENT SYSTEMS DEPARTMENT Table of Contents*.

Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 1–16.

Pham, M. T., & Nguyen, L. H. (2023). A Comparative Review of Cybersecurity Standards and Frameworks: Supporting Information Assurance in Government and Industry Systems. *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems*, *13*(8), 1–15.

Rusydi, M. T. (2024). Evaluating Global Cybersecurity Laws: Efectiveness of Legal Frameworks and Enforcement Mecanism in the Digital Age. *Walisongo Law Review (Walrev)*, *6*(1), 71–83.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, *5*(4), 533–561.

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, *17*(7), 324–334.