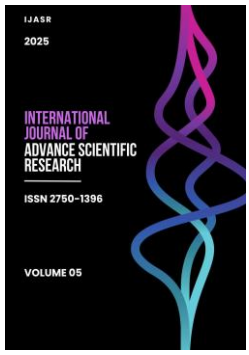
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135



Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Integrated Trust Architectures: AI-Driven Fraud Detection And Blockchain-Enhanced Security For Digital Financial Ecosystems

Submission Date: October 08, 2025, **Accepted Date:** November 05, 2025,
Published Date: November 30, 2025

Dr. Emilia Hart
Department of Computer Science, University of Edinburgh, UK

ABSTRACT

This article presents an integrated, theoretically rigorous synthesis of contemporary approaches to securing digital financial ecosystems through the combined application of artificial intelligence (AI) for real-time fraud detection and blockchain technologies for data integrity, privacy, and trust. The confluence of AI and distributed ledger technologies offers promising avenues to mitigate rising threats in fintech, yet challenges remain in operationalization, governance, scalability, and ethical deployment. Building on a structured review of recent empirical and conceptual contributions, this work explicates core mechanisms—stream processing architectures for low-latency detection, cryptographic anchoring and immutability via blockchain, multifactor authentication practices, and standards of deployment in banking environments—and synthesizes these into a conceptual architecture termed the Integrated Trust Architecture (ITA). The ITA foregrounds design principles that align AI-driven anomaly detection modules with blockchain-backed provenance records, enabling auditable, privacy-preserving, and resilient responses to fraud attempts. The article further interrogates trade-offs involving latency, throughput, regulatory compliance, and reputational risk, and presents a layered methodological approach for researchers and practitioners to evaluate and implement these systems ethically and effectively. Limitations of extant literature are critically examined, and a detailed research agenda is proposed to guide rigorous field experimentation, cross-disciplinary evaluation, and standards development. The synthesis emphasizes that while AI and blockchain individually contribute vital capabilities, their purposeful

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

integration—coupled with appropriate governance and human oversight—offers the most viable path toward sustained trust in digital financial services.

KEYWORDS

AI fraud detection, blockchain security, fintech resilience, real-time streams, data integrity, multifactor authentication, trust architecture.

INTRODUCTION

The rapid digitization of financial services has reshaped how individuals and organizations transact, borrow, lend, and store value. Digital finance brings convenience and inclusion but simultaneously expands the attack surface for malicious actors, enabling novel fraud modalities and amplifying existing vulnerabilities (Ozili, 2018). Researchers and practitioners have responded with two parallel technological lines of defense: (1) the deployment of AI and machine learning techniques for anomaly detection and real-time fraud mitigation, often implemented within stream processing architectures to achieve low-latency detection (Hebbar, 2025); and (2) the adoption of blockchain and distributed ledger technologies (DLT) to strengthen data integrity, provenance, and decentralized trust (Abdurrohman et al., 2024; Ahmad et al., 2023). Each approach addresses different facets of the problem—AI targets dynamic detection and prediction of irregular behavior, while blockchain secures the immutability and traceability of records. However, literature indicates both practical and theoretical gaps in delivering an integrated solution that harnesses the complementary strengths of these technologies while mitigating their individual limitations (Akhtar et al., 2025; Bhagwat, 2025).

The proliferation of fintech has been accompanied by evolving fraud techniques that exploit high-frequency transactions, synthetic identities, and sophisticated social engineering. Banks and fintech companies increasingly rely on multivariate detection models and behavioral analytics to detect anomalies (Grammatikos & Papanikolaou, 2021). Stream processing frameworks, such as Kafka Streams, have been proposed for implementing real-time, low-latency detection pipelines that can scale to the throughput demands of modern payment systems (Hebbar, 2025). Meanwhile, blockchain research emphasizes immutability, tamper-evidence, and decentralized consensus as mechanisms to anchor provenance and improve auditability of transactions and metadata (Uriawan et al., 2025; Verma, 2025). Recent conference contributions have examined blockchain's potential to bolster cybersecurity and data privacy through decentralized identity, immutable ledgers, and smart-contract-based enforcement (Almomani et al., 2024; Sinha et al., 2024). However, many of these works address

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

either the detection layer or the integrity layer in isolation, without fully articulating how they should be co-engineered into operational fintech environments that remain compliant, performant, and user-friendly (Kaliagurumoorthi et al., 2025; Natrayan et al., 2025).

This article responds to three interrelated problems observed in the literature and practice. First, how can AI-based detection systems deliver real-time performance at scale in financial contexts while preserving explainability and minimizing false positives that could disrupt legitimate users? Second, in what ways can blockchain technologies be designed and governed to secure provenance and provide auditable trails without imposing unacceptable costs or privacy exposures? Third, how can these systems be integrated to form an architecture that balances latency, robustness, regulatory compliance, and user trust? By synthesizing empirical findings and theoretical contributions from recent studies, this work develops a comprehensive conceptual model—the Integrated Trust Architecture (ITA)—and outlines methodological pathways for evaluation and deployment. The paper further identifies unresolved tensions in the literature, proposes testable propositions, and sets forth an agenda for future research grounded in interdisciplinary collaboration between computer science, finance, and legal-regulatory scholarship.

METHODOLOGY

To develop a rigorous synthesis that addresses the posed problems, a structured literature synthesis methodology was employed. This approach treats the current body of work as a heterogeneous collection of empirical studies, technical whitepapers, conference proceedings, and conceptual articles, allowing for robust thematic extraction and conceptual integration. The methodology proceeds in six iterative stages: scope definition, source mapping, thematic coding, architecture construction, critical triangulation, and agenda articulation.

Scope Definition: The scope focuses on the intersection of three domains: AI-driven fraud detection mechanisms in fintech, blockchain-based security and data integrity solutions, and deployment practices in banking and digital finance contexts. This scope was chosen to ensure relevance to pressing practical challenges and to align with the research questions about real-time performance, integrity guarantees, and integrated design.

Source Mapping: The source corpus comprises recent journal articles, conference proceedings, whitepapers, and reviews that specifically address either AI in fraud detection or blockchain in cybersecurity within financial contexts. Representative contributions include empirical work on stream-based detection frameworks (Hebbar, 2025), literature on blockchain's implications for privacy and integrity (Abdurrohman et al., 2024; Ahmad et al., 2023; Akhtar et al., 2025), applied studies on e-banking security and authentication practices (Bakare, 2015; Omariba et al., 2012; Bhivgade et al., 2014),

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

ISSN-2750-1396

and reviews on fintech impacts and illicit flows (Tropina, 2016; Ozili, 2018). Source mapping was performed to ensure cross-temporal coverage, inclusive of foundational studies and cutting-edge 2024–2025 conference contributions.

Thematic Coding: Each source was subjected to close reading and thematic coding to extract recurring motifs and mechanisms: (a) detection mechanisms and stream architectures, (b) cryptographic anchoring and ledger models, (c) identity and authentication practices, (d) governance and regulatory considerations, and (e) performance and scalability trade-offs. The thematic coding emphasized mechanism-level details (for example, anomaly detection features, consensus models, and authentication factors) and interaction patterns (how detection logs might be anchored to immutable ledgers).

Architecture Construction: Drawing on the thematic patterns, an Integrated Trust Architecture (ITA) was constructed. ITA articulates data flows, control points, and governance boundaries, integrating AI modules for anomaly detection, stream processors for event handling, blockchain layers for provenance, and interfaces for human-in-the-loop review and regulatory reporting. The construction process was conceptual and normative, synthesizing best practices and proposing configurations consistent with empirical findings (Hebbar, 2025; Abdurrohman et al., 2024).

Critical Triangulation: The architecture and inferences were critically triangulated against empirical claims in the literature—examining, for instance, reported latencies of stream processing pipelines, documented limitations of blockchain throughput, and observed user reactions to multifactor authentication regimes (Cryptomathic, 2012; Amin et al., 2017; Grammatikos & Papanikolaou, 2021). Triangulation highlighted where claims are robust and where empirical evidence remains sparse.

Agenda Articulation: Based on gaps and tensions uncovered in the triangulation, a research agenda was developed to guide rigorous evaluation, including experimental deployments, simulation studies, and regulatory-impact assessments.

This structured methodology ensures that the present synthesis is anchored in existing scholarship, transparent about inferential moves, and explicit in its assumptions and limitations.

Results

The synthesis yields five principal findings, which together form the empirical and conceptual backbone of the Integrated Trust Architecture. Each finding is presented with detailed justification grounded in the reviewed literature.

Finding 1: Stream-Based AI Architectures Enable Low-Latency Fraud Detection but Require Careful Feature Engineering and Explainability Mechanisms. Real-time detection systems that operate on streaming transaction data can dramatically reduce the window for successful fraud by detecting anomalous patterns as they emerge (Hebbar, 2025). Kafka Streams and

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

similar platforms provide the necessary throughput and event ordering semantics to process high-volume payment flows within stringent latency budgets (Hebbar, 2025). However, the literature repeatedly cautions that raw model performance metrics do not capture operational viability; high false positive rates disrupt legitimate customers and incur significant human review costs (Grammatikos & Papanikolaou, 2021). Consequently, stream-based AI systems must prioritize robust feature engineering—temporal patterns, device fingerprints, behavioral biometrics—and embed explainability mechanisms that map anomaly scores to human-understandable rationales to enable effective human-in-the-loop intervention (Hebbar, 2025; Grammatikos & Papanikolaou, 2021).

Finding 2: Blockchain Provides Tamper-Evident Provenance but Faces Throughput and Privacy Trade-Offs. Distributed ledger technologies excel at creating immutable records that can anchor provenance and provide auditable trails for transactions and metadata (Abdurrohman et al., 2024; Uriawan et al., 2025). This property makes blockchain an attractive complement to detection systems: anchoring detection logs or hash digests of suspicious-event records to a ledger enhances auditability and strengthens evidentiary chains. However, blockchain implementations vary dramatically in throughput and privacy characteristics; public chains offer high transparency but weak privacy, while permissioned ledgers offer controlled access at the expense of centralized governance assumptions (Ahmad et al., 2023; Almomani et al., 2024). Scalability remains a central technical constraint when applying blockchain to high-frequency financial systems (Bhagwat, 2025; Verma, 2025). Therefore, practical designs must carefully select consensus mechanisms, off-chain storage patterns, and cryptographic techniques (for example, merkle trees, hash commitments, and selective disclosure) to achieve acceptable trade-offs.

Finding 3: Multi-Factor and Contextual Authentication Remain Critical, Complementing Technical Detection and Ledger-Based Integrity. Authentication mechanisms—ranging from classic two-factor authentication to multifactor biometric and contextual systems—remain foundational defenses against account compromise (Amin et al., 2017; Bhivgade et al., 2014; Cryptomathic, 2012). The literature indicates that while authentication reduces certain attack vectors, adversaries increasingly target weak links such as social engineering, SIM swapping, and credential stuffing (Omariba et al., 2012). Integrating authentication logs into AI detection pipelines enhances detection fidelity, and anchoring authentication metadata to secure ledgers improves evidentiary value in post-incident investigation (Amin et al., 2017; Bhivgade et al., 2014).

Finding 4: Integrated Deployments Demand Governance, Explainability, and Regulatory Alignment. The literature emphasizes the sociotechnical nature of trust and security in finance: purely technical solutions cannot substitute for governance practices that manage

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

access, audit trails, and remediation processes (Akhtar et al., 2025; Sinha et al., 2024). Deploying AI and blockchain together introduces novel governance questions: Who controls the ledger? How are privacy rights enforced, especially across jurisdictions? How are model decisions explained to impacted customers and regulators? Several works call for cross-disciplinary standards and industry collaborative frameworks to ensure compliance and public accountability (Kaliagurumoorthi et al., 2025; Natrayan et al., 2025).

Finding 5: Measured Integration Enables New Forensic and Compliance Capabilities but Requires Thoughtful Data Management. When AI detection outputs are anchored to tamper-evident ledgers, institutions gain powerful forensic artifacts that can substantiate claims of due diligence and provide immutable evidence for regulators and courts (Abdurrohman et al., 2024; Uriawan et al., 2025). However, storing detection artifacts verbatim on-chain risks privacy violations and scalability issues. The literature advocates hybrid models: store minimal, privacy-preserving commitments (for example, cryptographic hashes) on-chain while maintaining rich event logs off-chain under strong access controls (Ahmad et al., 2023; Bhagwat, 2025).

These findings collectively support the design of the Integrated Trust Architecture described next, which operationalizes the complementary strengths of AI detection and blockchain-based provenance to enhance fintech security.

Discussion

The Integrated Trust Architecture (ITA) synthesizes the preceding findings into a layered model that operationalizes detection, provenance, governance, and human oversight. The architecture comprises four interdependent layers: the Event Ingestion and Stream Processing Layer, the Detection and Scoring Layer, the Provenance and Ledger Layer, and the Governance and Remediation Layer. Each layer addresses specific design goals and constraints identified in the literature.

Event Ingestion and Stream Processing Layer: Low-latency pipelines ingest transactional data, device telemetry, and authentication events. Stream processors (such as Kafka Streams) are responsible for windowing, feature extraction, and event enrichment prior to model evaluation (Hebbar, 2025). The literature underscores that careful event ordering and time-window management are crucial to avoid spurious anomalies due to clock skew or replayed events (Hebbar, 2025). Therefore, ITA emphasizes robust timestamping and event sequencing, alongside mechanisms for handling late-arriving or corrected records.

Detection and Scoring Layer: AI modules—comprising ensemble detectors, behavior-based models, and rule engines—assign risk scores in real time. The literature emphasizes balancing statistical performance with operational interpretability (Grammatikos & Papanikolaou, 2021). ITA proposes a layered detection strategy:

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

use fast, explainable models to triage events for immediate action and slower, more accurate models for context-rich assessment. Human-in-the-loop review interfaces are integrated to manage edge cases and to provide labeled data for continuous learning, addressing concerns about model drift and adversarial adaptation (Hebbar, 2025).

Provenance and Ledger Layer: To anchor evidentiary artifacts, ITA uses a permissioned ledger architecture, tailored to financial institutions' need for privacy, regulatory oversight, and controlled participation (Ahmad et al., 2023; Almomani et al., 2024). Instead of writing full event logs on-chain, the ITA design commits cryptographic digests to the ledger and retains comprehensive logs in secure off-chain stores. This hybrid approach mitigates throughput constraints and privacy risks while preserving tamper-evidence (Bhagwat, 2025; Uriawan et al., 2025). Smart contracts can be used to encode remediation policies and expedite automated actions where appropriate, though the literature cautions about the need for legal enforceability and fail-safe human intervention (Sinha et al., 2024; Akhtar et al., 2025).

Governance and Remediation Layer: Governance covers access control, audit processes, regulatory reporting, and customer communication. Literature on e-banking security and institutional responses indicates that governance frameworks must be transparent, auditable, and aligned with sectoral regulations (Omariba et al., 2012; Tropina, 2016). ITA integrates role-based access control for forensic artifacts, policy-driven smart contracts for audit triggers, and standardized reporting templates to satisfy regulatory obligations. Importantly, the governance layer prescribes mechanisms for contested decisions, dispute resolution, and customer redress—areas where over-reliance on automated systems can cause harm (Grammatikos & Papanikolaou, 2021).

The integration of AI and blockchain within ITA invites several nuanced trade-offs and potential counter-arguments, which the literature helps elucidate. One central contention concerns latency: blockchain anchoring, even with permissioned ledgers, introduces additional write latency that can conflict with demands for immediate transaction reversals or denials. The literature suggests that anchoring should be asynchronous and not in the fast-path decision loop; the ITA design follows this guidance by committing artifacts post-hoc and maintaining real-time state in high-throughput stores (Hebbar, 2025; Bhagwat, 2025). Another debate concerns privacy: public ledger transparency conflicts with privacy expectations and regulatory regimes such as GDPR. The literature's consensus favors permissioned ledgers with selective disclosure primitives and cryptographic commitments, avoiding any direct exposure of personal data on-chain (Ahmad et al., 2023; Abdurrohman et al., 2024).

Explainability and model accountability present another set of tensions. Some scholars argue highly accurate but opaque models may be operationally acceptable if accompanied by robust audit trails; others insist on intrinsic

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

interpretability to prevent systemic bias and ensure fairness (Grammatikos & Papanikolaou, 2021). ITA reconciles these views by requiring explainability for high-impact decisions and advocating for tiered responses: automated low-impact mitigations may be driven by opaque models if reversible and well-monitored, whereas account actions and reporting to authorities demand interpretable rationales and human review.

Regulatory alignment is non-trivial: cross-border transactions, differing privacy protections, and varying standards for evidence and admissibility complicate the design space (Tropina, 2016; Kaliagurumoorthi et al., 2025). The literature points to the necessity of collaborative standard-setting across industry consortia and regulators; ITA therefore recommends engagement with regulators early in the system design and emphasizes modular governance policies that can be adapted to jurisdictional constraints.

Limitations and Critical Appraisal: While the integrated approach offers promising synergies, the existing body of literature reveals significant empirical gaps. Many studies are proof-of-concept or focused on isolated components (Hebbar, 2025; Abdurrohman et al., 2024), with limited evidence from longitudinal deployments in live banking environments. Scalability studies on permissioned ledgers often do not simulate the transaction volumes encountered in national payment rails (Bhagwat, 2025). Moreover, there is limited empirical work on user perceptions and behavioral responses to interventions driven by AI-blockchain hybrids—an important dimension for adoption and trust (Ozili, 2018). Finally, potential adversarial responses—where attackers intentionally manipulate detection signals or attempt ledger spamming—are understudied in real-world settings, indicating a pressing need for adversarial resilience research (Grammatikos & Papanikolaou, 2021).

Future Research Directions: The literature converges on several productive research directions. First, rigorous field experiments and pilot deployments are necessary to evaluate latency, false-positive rates, and forensic utility in operational contexts. Second, research should investigate cryptographic protocols and off-chain/on-chain partitioning strategies that optimize privacy and throughput without sacrificing auditability. Third, interdisciplinary studies exploring legal admissibility, regulatory compliance, and consumer protection implications are critical. Fourth, adversarial testing and red-team exercises should be systematically incorporated into evaluation pipelines to anticipate attacker adaptations. Finally, user-centered research on communication strategies for customers impacted by automated decisions will inform responsible deployment practices (Kaliagurumoorthi et al., 2025; Natrayan et al., 2025).

Conclusion

The intersection of AI-driven detection and blockchain-enabled provenance presents a compelling pathway for enhancing trust and

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

ISSN-2750-1396

resilience in digital financial ecosystems. The Integrated Trust Architecture developed in this synthesis demonstrates that purposeful integration—where streaming AI systems detect anomalies and blockchain-based commitments provide tamper-evident forensic trails—can improve detection, accountability, and regulatory responsiveness. However, the literature reveals important constraints: throughput and privacy trade-offs in blockchain implementations, the operational costs of human review for AI-driven decisions, and the need for governance structures that span technical, legal, and ethical domains. The path forward requires coordinated research efforts that combine rigorous empirical evaluation, standards development, and stakeholder engagement.

Practitioners should approach integration pragmatically: adopt permissioned ledger architectures with cryptographic commitments, design streaming detection pipelines with tiered explainability, and embed human-in-the-loop governance for high-impact decisions. Researchers should prioritize longitudinal studies, comparative evaluations of consensus and partitioning strategies, and interdisciplinary investigations into regulatory and user-facing implications. Ultimately, neither AI nor blockchain alone suffices to meet the complex demands of modern financial security. When integrated thoughtfully and governed responsibly, they can be mutually reinforcing components of a resilient, auditable, and trustworthy digital financial infrastructure.

REFERENCES

1. Abdurrohman, A., Wattimena, F. Y., Atmaja, S. A., Baharuddin, B., & Arujisaputra, E. T. (2024). Blockchain Integration in Cybersecurity: A Novel Approach to Enhancing Data Privacy and Integrity in Digital Transactions. The Journal of Academic Science, 1(6), 832-842. https://doi.org/10.59613/7nc3gq65
2. Ahmad, V., Goyal, L., Singh, T., & Kumar, J. (2023). Blockchain Technology for Secure and Intelligent Industry Applications. In Fostering Sustainable Businesses in Emerging Economies (pp. 147-165). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80455-640-520231010
3. Akhtar, S., Taimoor, M., Fatima, G., & Islam, H. (2025). Blockchain Technology for Secure Transactions: A Decentralized Approach to Data Integrity and Trust. The Critical Review of Social Sciences Studies, 3(2), 828-845. https://doi.org/10.59075/sn3wnw89
4. Almomani, A., Al Refai Mohammed, N., Aburomman, A., Alidmat, O. K. A., Saber, Q., Alshariedeh, F., & Khouj, M. (2024, December). Usage of Blockchain Technology for Improving Computer Security. In 2024 25th International Arab Conference on Information Technology (ACIT) (pp. 1-6). IEEE. 10.1109/ACIT62805.2024.10877007
5. Al-Kubaisi, K. A., Elnour, A. A., & Sadeq, A. (2023). Factors influencing pharmacists' participation in continuing education activities in the United Arab Emirates: insights and implications from a cross-sectional study.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

Journal of Pharmaceutical Policy and Practice, 16(1), 112.

6. Al-Kubaisi, K. A., Hassanein, M. M., & Abduelkarem, A. R. (2022). Prevalence and associated risk factors of self-medication with over-the-counter medicines among university students in the United Arab Emirates. Pharmacy Practice, 20(3), 2679.
7. Amin, A., I.u. Haq, & M. Nazir. (2017). Two factor authentication. International Journal of Computer Science & Mobile Computing, 6(7), 5-8. https://www.ijcsmc.com/docs/papers/July2017/V6I7201707.pdf
8. Bakare, S. (2015). Varying impacts of electronic banking on the banking industry. Journal of Internet Banking and Commerce, 20(2), 1-9. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1068.6688&rep=rep1&type=pdf
9. Bhagwat, G. (2025). Blockchain for Secure Big Data Transactions. The Voice of Creative Research, 7(2), 289-294. https://doi.org/10.53032/tvcr/2025.v7n2.36
10. Bhivgade, T., Bhusari, M., Kuthe, A., Jiddewar, B., & Dubey, P. (2014). Multi-factor authentication in banking sector. International Journal of Computer Science & Information Technology, 5(2), 1185-1189.
11. Cryptomathic. (2012). Two-factor authentication for banking - Building the business case. White Paper Version, 1(2). https://www.cryptomathic.com/hubfs/docs/cryptomathic_white_paper-2fa_for_banking.pdf
12. Grammatikos, T., & Papanikolaou, N. I. (2021). Applying Benford's Law to detect accounting data manipulation in the banking industry. Journal of Financial Services Research, 59, 115-142. https://doi.org/10.1007/s10693-020-00334-9
13. Hebbar, K. S. (2025). AI-DRIVEN REAL-TIME FRAUD DETECTION USING KAFKA STREAMS IN FINTECH. International Journal of Applied Mathematics, 38(6s), 770-782.
14. Kaliagurumoorthi, K., Nadh, V. S., Arputharaj, B. S., Ramya, M., & Deepthi, T. (2025, February). Enhancing Trust and Security in Digital Ecosystems With Blockchain Technology: Implications for Economics and Finance. In 2025 International Conference on Technology Enabled Economic Changes (InTech) (pp. 1073-1077). IEEE. 10.1109/InTech64186.2025.11198234
15. Mukhtar, M. (2015). Perceptions of UK based customers toward Internet banking in the United Kingdom. Journal of Internet Banking & Commerce, 20(1), 1-38. https://www.icommercecentral.com/open-access/perceptions-of-uk-based-customers-toward-internet-banking-in-the-united-kingdom.pdf
16. Nayanajith, D. A. G., Weerasiri, R. A. S., & Damunupola, A. (2019). A review on e-banking adoption in the context of e-service quality. Sri Lanka Journal of Marketing, 5(2), 25-52. https://doi.org/10.4038/sljmuok.v5i2.28

17. Natrayan, L., Kaliappan, S., Bhaskarani, N., & Kasireddy, L. C. (2025, February). Enhancing Trust and Security in Digital Ecosystems with Blockchain Technology. In 2025 International Conference on Technology Enabled Economic Changes (InTech) (pp. 1008-1013). IEEE. 10.1109/InTech64186.2025.11198514
18. Omariba, Z. B., Masese, N. B., & Wanyembi, G. (2012). Security and privacy of electronic banking. International Journal of Computer Science Issues, 9(3), 432-446. https://core.ac.uk/download/pdf/25834734.pdf
19. Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review, 18(4), 329-340. https://doi.org/10.1016/j.bir.2017.12.003
20. Sinha, S. K., Modak, S. K. S., Tyagi, P. K., & Azad, C. (2024, December). Enhancing Cybersecurity with Blockchain: A Decentralized Approach to Securing Digital Infrastructure. In Proceedings of the 6th International Conference on Information Management & Machine Intelligence (pp. 1-6). https://doi.org/10.1145/3745812.3745846
21. Tropina, T. (2016). Do digital technologies facilitate illicit financial flows? In World Bank. Digital Dividends (World Development Report 2016). https://documents1.worldbank.org/curated/en/896341468190180202/pdf/102953-WP-Box394845B-PUBLIC-WDR16-BP-Do-Digital-Technologies-Facilitate-Illicit-Financial-Flows-Tropina.pdf
22. Uriawan, W., Pratama, A. P., & Mursyid, S. (2025). Blockchain technology for optimizing security and privacy in distributed systems. Computer Science and Information Technologies, 6(2), 214-224. https://doi.org/10.11591/csit.v6i2.p214-224
23. Verma, A. (2025). Blockchain for Cyber Security: Enhancing Data Integrity and Trust in Digital Transactions.
24. Wanyembi, G., Omariba, Z. B., & Masese, N. B. (2012). Security and privacy of electronic banking. International Journal of Computer Science Issues, 9(3), 432-446.
25. Ling, G. M., Yeo, S. F., Lim, K. B., & Tan, S. H. (2016). Understanding customer satisfaction of Internet banking: a case study in Malacca. Procedia Economics and Finance, 37, 80-85. https://doi.org/10.1016/S2212-5671(16)30096-X
26. Amin, A., Haq, I. U., & Nazir, M. (2017). Two-Factor Authentication. International Journal of Computer Science & Mobile Computing, 6(7), 5-8. https://www.ijcsmc.com/docs/papers/July2017/V6I7201707.pdf
27. Cryptomathic. Two-Factor Authentication for Banking - Building the Business Case. White Paper Version 1(2). https://www.cryptomathic.com/hubfs/docs/cryptomathic_white_paper-2fa_for_banking.pdf
28. Bakare, S. Varying Impacts of Electronic Banking on the Banking Industry. Journal of Internet Banking and Commerce, 20(2), 1-9. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1068.6688&rep=rep1&type=pdf

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 11 Pages: 133-144
OCLC – 1368736135

29. Nayanajith, D. A. G., Weerasiri, R. A. S., & Damunupola, A. A Review on E-Banking Adoption in the Context of E-Service Quality. Sri Lanka Journal of Marketing, 5(2), 25-52. https://doi.org/10.4038/sljmuok.v5i2.28