

Assuring Information Integrity in Mobile Cloud Computing: A Multi-Level Transaction Security Approach

¹Tajudeen Olanrewaju Toyib; ²Sikirullah Abdussomad Olose

¹Department of Computer Science, Al-Hikmah University Ilorin, Kwara Nigeria

²Department of Computer Science, Al-Hikmah University Ilorin, Kwara Nigeria

Corresponding Author's Email: toyibolanrewajutajudeen@gmail.com

Received on: August, 2026

Revised and Accepted on: September, 2026

Published on: October, 2026

ABSTRACT

The spread of mobile cloud computing has made data integrity harder to guarantee. Transmitting data across distributed, resource-constrained environments exposes it to corruption, interception, and makes the transaction not complete in ways that existing single-layer security mechanisms do not adequately address. Encryption, blockchain, and provable data possession each target distinct points in the data lifecycle; none protects the full transaction. This study applies design science research to identify those limitations and to build a multi-layer transaction security framework that addresses them directly. The framework is organised around four interdependent components: identity authentication, data verification, fault tolerance, and efficiency optimisation. Testing was conducted in a simulation environment configured with 100 mobile devices, five cloud nodes, and 5,000 transactions across three scenario types. The framework achieved a 96% data integrity rate, compared with 85% for traditional encryption models. Transaction latency was 1.8 seconds, against 2.5 seconds for blockchain-only systems. Reliability under fault conditions reached 94%. The results support the case for integrated, lifecycle-aware security architectures in mobile banking, healthcare, and Internet of Things (IoT) deployments.

Keywords: Mobile cloud computing, information integrity, transaction security, data validation, fault tolerance

1.0 INTRODUCTION

Mobile cloud computing has become central to contemporary digital infrastructure. It allows mobile devices to offload computationally intensive tasks to remote cloud servers, maintaining accessibility and scalability across sectors that include healthcare, financial services, smart cities, and industrial monitoring (Muhammad, 2024). But the dynamic, decentralised, and multi-party character of these environments creates persistent vulnerabilities. Data integrity, defined as the assurance that information remains accurate, consistent, and unaltered throughout its lifecycle (Yong, 2024), is difficult to guarantee precisely because the architecture that makes mobile cloud computing useful is the same architecture that makes it susceptible.

The problem is structural. Unlike conventional cloud systems anchored to stable networks, mobile cloud computing runs through intermittent connectivity, heterogeneous devices, edge nodes, and IoT sensors that continuously generate and exchange data across poorly controlled channels (Chao, 2022). Tampering, interception, corruption, and transaction incompleteness all follow from these conditions. Conventional security models, designed for stable, centralised environments, do not address them adequately (Qayyum & Ejaz, 2020). Existing solutions compound the difficulty: cryptographic methods such as provable data possession offer strong storage-level assurances but leave transactions in transit unprotected (Luo et al., 2022); blockchain-based approaches

improve decentralised trust but introduce latency and energy overheads that mobile devices cannot sustain (Vallu et al., 2025); and lightweight schemes sacrifice security depth to gain efficiency (Hussien et al., 2023). Each approach fills one gap while creating another.

Two objectives guide this study: (1) to examine existing techniques for ensuring data integrity in mobile cloud computing and identify their limitations; and (2) to design and evaluate a multi-level transaction security framework for assuring information integrity in mobile cloud environments. The framework draws on Information Assurance Theory (Whitman & Mattord, 2018), which insists that security must be proactive and never reducible to a single mechanism; Defence in Depth Theory (Anderson, 2008), which requires that multiple independent controls be layered so that the failure of one does not compromise the whole; and the Zero Trust Security Model (Kindervag, 2010), which holds that no user or device should be trusted by default and that verification must be continuous. Together these frameworks argue for the integrated, lifecycle-spanning approach developed here.

2.0 LITERATURE REVIEW

2.1 Mobile Cloud Computing and the Integrity Problem

Mobile cloud computing extends mobile device capability by offloading processing, memory, and battery-intensive tasks to cloud infrastructure (Muhammad, 2024). The gains in scalability and

accessibility are real, but they come at a cost: network connectivity fluctuates, devices move through multiple access points, and data passes through layers that neither users nor organisations directly control (Luo et al., 2022). The attack surface this creates is wider than perimeter-based security models were ever designed to handle. IoT integration stretches it further still. Smart meters, wearable sensors, and industrial monitors generate continuous streams of cloud-bound data in environments where physical security cannot always be assured (Zhou & Wang, 2022).

The scale of the problem is not academic. In a systematic review of 146 studies, Albshaier et al. (2024) found that authentication weaknesses appeared in 41% of paper and data integrity issues in 38%, confirming that neither concern has been resolved to the field’s satisfaction. Global figures from the International Telecommunication Union (2024) placed mobile broadband traffic at approximately 1.3 zettabytes in 2024, with 112 mobile cellular subscriptions per 100 inhabitants worldwide and 68% of the global population online. The World Bank (2025) reported that mobile cellular subscriptions exceed population ratios in most regions. At that density of use, security weaknesses that seem marginal in isolation produce consequences that are not. Yet existing approaches continue to address isolated components of the problem rather than the full transaction lifecycle from data generation through transmission, validation, and storage (Goswami et al., 2024).

2.2 Existing Data Integrity Techniques and Their Limitations

Several categories of techniques have been proposed for data integrity in mobile cloud systems. Cryptographic methods, including AES and RSA encryption, SHA-256 hashing, and digital signatures, are among the most widely deployed (Phatangare, 2024; Shabbir et al., 2021). Digital signatures also supply non-repudiation, which matters specifically for financial and healthcare transactions (Leila et al., 2020). The limits, though, are worth stating plainly. Encryption protects confidentiality; it does not prevent data manipulation after decryption. Hashing detects tampering rather than preventing it and must be combined with other mechanisms to provide protection that is actually complete (Qayyum & Ejaz, 2020).

Provable data possession schemes take a different approach, allowing users to confirm data correctness without retrieving the full dataset. Extensions using lattice-based cryptography have made them resistant to quantum attacks (Luo et al., 2022; Zhao & Chen, 2025; Zhou et al., 2022). The gap that remains is a serious one: these schemes operate at the storage level and say nothing about what happens to data during active transmission (Wu et al., 2024). Blockchain-based models address decentralised trust and immutability but carry a cost in latency and energy consumption that resource-constrained mobile devices cannot absorb (Akbar et al., 2024; Shakor et al., 2024). Lightweight security schemes come closer to fitting mobile constraints but typically achieve efficiency by thinning out security depth (Hussien et al., 2023). Table 1 sets out these comparative limitations.

Table 1: Comparative Limitations of Existing Data Integrity Techniques

Technique	Integrity Coverage	Latency Impact	Mobile Suitability	Key Limitation
Encryption (AES/RSA)	Confidentiality only	Low	Moderate	Does not prevent post-decryption manipulation
SHA-256 Hashing	Detection only	Low	High	Detects but does not prevent tampering
Digital Signatures	Auth + Integrity	Moderate	Moderate	Key management complexity
Provable Data Possession	Storage level	Moderate	Low	Not applicable during active transactions
Blockchain Models	High	High	Low	Excessive latency and energy consumption

Lightweight Schemes	Partial	Low	High	Reduced security depth
---------------------	---------	-----	------	------------------------

Note: Sources: Akbar et al. (2024); Hussien et al. (2023); Luo et al. (2022); Phatangare (2024); Shakor et al. (2024); Wu et al. (2024).

2.3 Theoretical Framework

Three theoretical frameworks inform the design of the proposed model. Information Assurance Theory (Whitman & Mattord, 2018) organises security around five core principles: confidentiality, integrity, availability, authentication, and non-repudiation. Security, on this account, must be proactive rather than reactive, and no single mechanism is ever sufficient in isolation. That premise directly supports a multi-level design in which authentication, validation, and fault tolerance function as interdependent components rather than standalone controls. Defence in Depth Theory (Anderson, 2008) extends this argument: independent security controls must be layered such that the failure of any one leaves the others intact. Applied to mobile cloud computing, where threats appear at device, network, and cloud layers, independent protection at each stage is not optional. The Zero Trust Security Model (Kindervag, 2010), formalised later by Rose et al. (2020), starts from a starker premise: no user or device should be trusted by default. In mobile cloud contexts, where devices move through access points and network boundaries shift dynamically, verification cannot be limited to the entry point. It must operate throughout the transaction. All three frameworks, read together, demand something the existing literature has not yet produced: a security architecture that covers the full transaction lifecycle.

2.4 Research Gap

Three gaps emerge from literature. No widely accepted model integrates authentication, validation, fault tolerance, and efficiency into a single transaction-lifecycle framework; studies have tended to address these components in isolation, which is precisely the condition that leaves mobile cloud data exposed. Fault tolerance and recovery mechanisms are largely absent from integrity-focused research, despite being essential for maintaining data consistency through the network disruptions that characterise mobile environments (Zaid *et al.*, 2023; Neoaz & Amin, 2025). And efficiency is rarely treated as a core security design variable, producing models that are either protective but impractical on mobile hardware, or efficient but

insufficiently protective (Hussien et al., 2023; Wang et al., 2023). The framework developed in this study is a direct response to all three.

3.0 FRAMEWORK DESIGN

3.1 Research Design

Design science research provides the methodological basis for this study. The approach is suited to work that aims to build and evaluate new systems or artefacts rather than analyse existing ones (Kothari, 2004), and the present study is squarely of that kind. Qualitative analysis of existing literature drove the identification of system requirements and shaped the framework architecture. Quantitative methods then governed simulation-based evaluation. A simulation environment was chosen because it permits controlled testing under conditions that approximate real-world mobile cloud challenges, without the cost and deployment constraints that full-scale industrial implementation would impose (Rajasekar & Verma, 2013).

3.2 Proposed Multi-Level Transaction Security Framework

Four security layers, integrated into a single architecture, protect data across the full transaction lifecycle. Each targets a distinct category of vulnerability identified in the literature review. The authentication layer verifies user and device identity through multi-factor authentication (MFA), token-based verification, and biometric methods, so that only authorised parties can initiate transactions (Wang et al., 2023). Accuracy during and after transmission is the concern of the data validation layer, which applies SHA-256 hashing, digital signatures, and checksum comparison (Phatangare, 2024). The fault tolerance layer uses checkpointing and data replication to hold integrity through network disruptions, recovering incomplete transactions without data loss (Zaid et al., 2023). And where the other layers are protective, the efficiency optimization layer is enabling lightweight encryption and selective security activation keep the system usable on resource-constrained mobile devices (Hussien et al., 2023). Figure 1 presents the full framework.

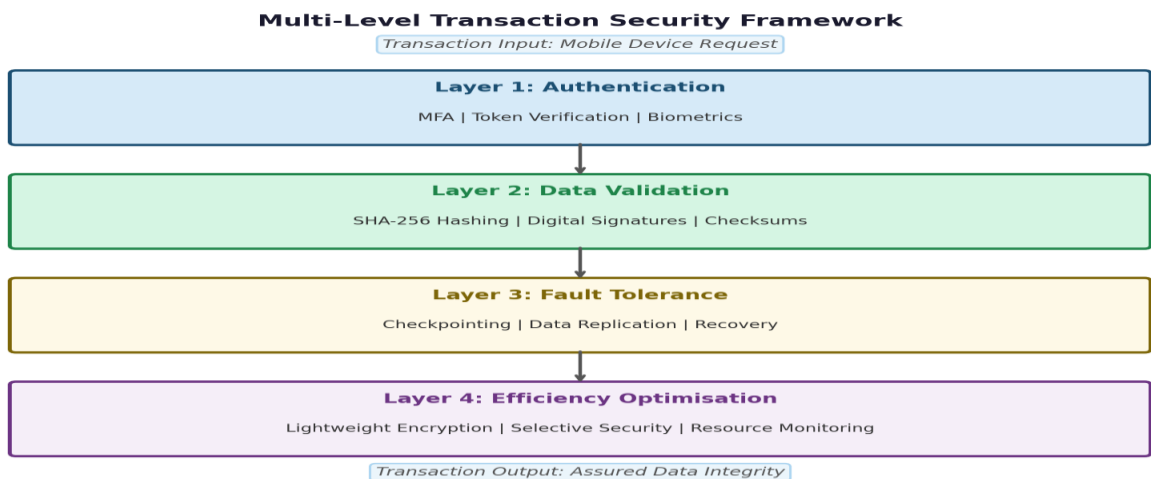


Figure 1: Multi-Level Transaction Security Framework Showing Four Integrated Security Layers.

3.3 System Architecture

The architecture spans three domains. At the mobile layer, 100 simulated mobile devices and IoT sensor nodes generate transaction requests; authentication is applied here, at the point of initiation. The network layer handles secure transmission through encrypted channels and manages fault recovery when interruptions occur. Five virtual cloud nodes form the

cloud layer, where data validation, processing, and secure storage take place, with integrity verification operating as a final check before data is committed. Figure 2 traces the transaction process flow from initiation to completion, including the failure and recovery path that the fault tolerance mechanism manages. Figure 3 shows how the three domains interact.

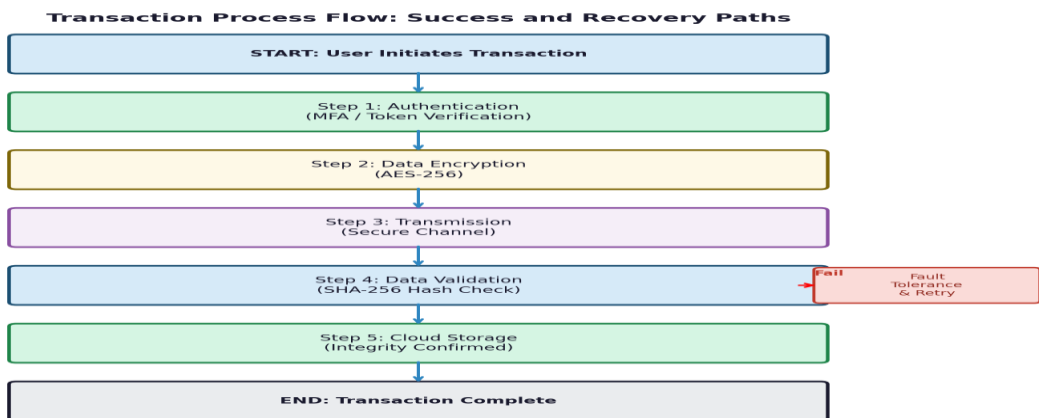


Figure 2: Transaction Process Flow Showing Success Path and Fault Tolerance Recovery Path.

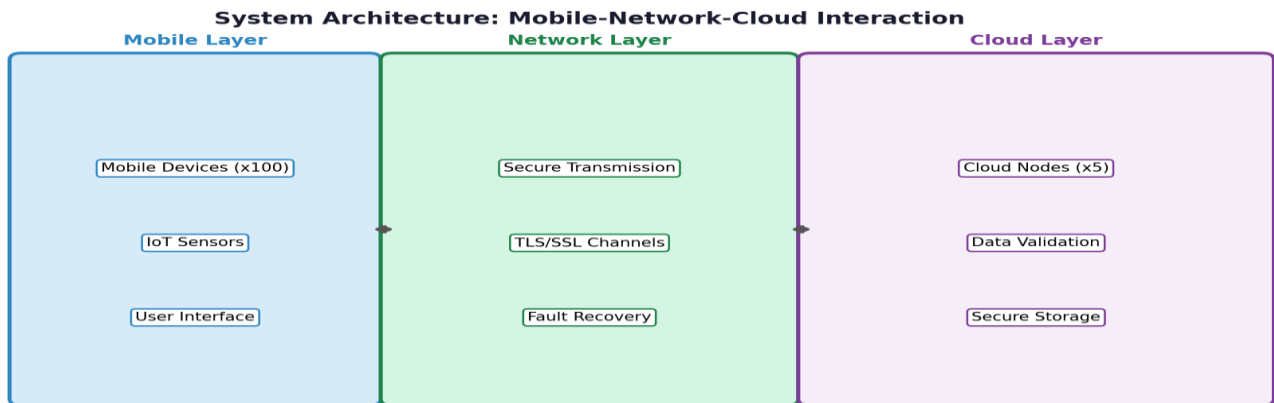


Figure 3: System Architecture Showing Interaction Between Mobile, Network, and Cloud Layers.

3.4 Algorithms and Tools

Algorithm selection was driven by fitness for mobile constraints. AES-256 was chosen for data protection

during transmission; its efficiency and adoption in mobile security environments are well established (Phatangare, 2024). For integrity verification, SHA-

256 hashing produces unique, tamper-evident outputs with low computational overhead, which makes it workable on mobile devices (*Shabbir et al., 2021*). RSA supplied digital signature generation and, with it,

non-repudiation. Python served as the simulation language, chosen for its flexibility and its support for cryptographic libraries. Table 2 sets out the simulation tools and their functions.

Table 2: Simulation Tools, Algorithms and Functions

Tool / Algorithm	Type	Function in Framework
AES-256	Symmetric encryption	Data protection during transmission
SHA-256	Cryptographic hash	Integrity verification before and after transmission
RSA-2048	Asymmetric encryption	Digital signature generation and non-repudiation
Python 3.10	Simulation language	Framework modelling, scenario testing, and metric calculation
Virtual Cloud Nodes	Infrastructure simulation	Data processing, validation, and secure storage
MFA Module	Authentication protocol	Multi-factor identity verification at transaction initiation

Note: All algorithms were implemented within a controlled simulation environment to evaluate framework performance.

4.0 IMPLEMENTATION AND RESULTS

4.1 Simulation Environment and Test Scenarios

The simulation replicated a mobile cloud environment in which 100 mobile nodes generated transaction requests under both stable and unstable network conditions, directed to five cloud nodes for processing and storage. In all, 5,000 transactions ran across a 60-

minute window. Three scenarios structured the evaluation: normal operation (stable network, no attacks), network failure (interruptions during active transactions), and data tampering, in which unauthorised modification of transaction data was simulated. Table 3 sets out the full simulation parameters.

*Table 3:***Simulation Environment Parameters**

Parameter	Value
Number of mobile devices	100
Cloud nodes	5
Total transactions generated	5,000
Simulation duration	60 minutes
Network conditions tested	Stable and unstable (variable)
Test scenarios	Normal operation, network failure, data tampering
Performance metrics	Integrity rate, latency, energy consumption, reliability

Note. Analysis, 2026.

4.2 Performance Results

Four performance metrics structured the evaluation: integrity rate, latency, energy consumption, and reliability. Table 4 records the integrity rates by scenario. Normal operation returned the highest rate, at 98%; under stable conditions, the validation and authentication layers functioned without measurable

degradation. Network failure reduced that figure to 94%, marginally, which is the point: the fault tolerance mechanism recovered most interrupted transactions. Under data tampering conditions the rate held at 96%, confirming that SHA-256 hashing and digital signature validation reliably detected and rejected unauthorised modifications.

Table 4: Integrity Rate by Test Scenario

Test Scenario	Integrity Rate (%)	Primary Mechanism Active
---------------	--------------------	--------------------------

Normal operation	98	Authentication + Validation
Network failure	94	Fault Tolerance + Recovery
Data tampering	96	SHA-256 Hashing + Digital Signatures
Overall (weighted average)	96	Full Four-Layer Framework

Note. Analysis, 2026.

Table 5 summarises performance across all evaluated indicators. An overall latency of 1.8 seconds captures the combined overhead of authentication, encryption, transmission, and validation; that figure remains within acceptable thresholds for real-time mobile applications. Energy consumption was rated low, a

result that reflects the efficiency optimisation layer working as intended to reduce computational burden on mobile devices. System reliability across all scenarios was 94%, consistent even under disruptive conditions.

Table 5: Overall Framework Performance Metrics

Metric	Value	Interpretation
Integrity rate	96%	High; validation and fault tolerance-maintained data accuracy
Transaction latency	1.8 seconds	Acceptable for real-time mobile applications
Energy consumption	Low	Suitable for battery-constrained mobile devices
System reliability	94%	Stable performance maintained across all test scenarios

Note. Analysis, 2026.

4.3 Comparison with Existing Security Models

Table 6 places the proposed framework alongside two established alternatives: traditional single-layer encryption and blockchain-only models. At 96%, the proposed model’s integrity rate exceeded traditional encryption (85%); its latency of 1.8 seconds undercut

blockchain-only systems (2.5 seconds). Efficiency ratings were highest for the proposed model, attributable to the lightweight mechanisms in the efficiency optimisation layer. Figure 4 visualises all three dimensions together.

Table 6: Performance Comparison: Proposed Model Versus Existing Approaches

Security Model	Integrity Rate	Latency	Efficiency
Traditional encryption	85%	1.2 seconds	Moderate
Blockchain only	95%	2.5 seconds	Low
Proposed multi-level framework	96%	1.8 seconds	High

Note. Sources: Akbar et al. (2024); Shakor et al. (2024); Vallu et al. (2025). Analysis, 2026.

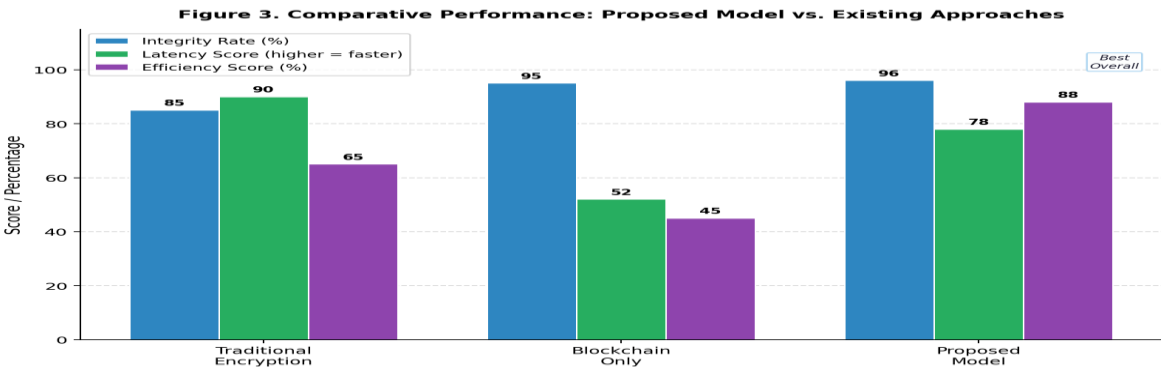


Figure 4: Comparative Performance of the Proposed Model Against Traditional Encryption and Blockchain-Only Approaches Across Integrity, Latency, and Efficiency Dimensions.

5.0 DISCUSSION

5.1 Existing Techniques and Their Limitations (Objective 1)

Single-layer mechanisms are not adequate for transaction-level integrity in mobile cloud environments. The simulation results make this concrete. Traditional encryption achieved an integrity rate of only 85%, a figure that reflects its inability to detect post-decryption manipulation or recover data corrupted during network interruptions. This is precisely the limitation Qayyum and Ejaz (2020) described when arguing that mobile cloud computing requires adaptive, layered solutions rather than static cryptographic controls. Blockchain-based models did better at 95%, but the latency of 2.5 seconds is a real constraint for banking, healthcare, and IoT applications that depend on real-time responses, a point consistent with Akbar et al. (2024) and Vallu et al. (2025).

Provable data possession and proof-of-retrievability methods are effective at storage-level verification, but they say nothing about what happens to data while it is actively moving between mobile devices and cloud servers (Luo et al., 2022; Wu et al., 2024; Zhao & Chen, 2025). In mobile environments, where network instability is common and transactions are routinely interrupted, this is not a minor gap (Zaid et al., 2023). Albshaier et al. (2024) found that data integrity concerns appear in nearly 40% of IoT-cloud security studies. The implication is clear enough: no existing single-method approach covers the full transaction lifecycle adequately, and the first objective of this study is validated on that basis.

5.2 Framework Design and Evaluation (Objective 2)

Security controls distributed across the full transaction lifecycle produce better outcomes than any single-layer approach. The authentication layer, implementing MFA and token verification, blocked unauthorised transaction initiation in a way that aligns with Wang et al.'s (2023) argument for adaptive, continuously verified identity management. Under active attack conditions, the data validation layer held integrity at 96%, using SHA-256 hashing and digital signatures; cryptographic verification did not degrade under pressure. That finding extends the work of Shabbir et al. (2021) and Phatangare (2024) by embedding validation within a multi-layer architecture rather than applying it as a standalone mechanism, which is precisely what those studies stopped short of doing.

The fault tolerance layer warrants particular attention. Under network failure conditions, the integrity rate fell only from 98% to 94%, which means checkpointing and data replication held transaction continuity through disruption rather than collapsing under it. This speaks

directly to the gap Neoaz and Amin (2025) and Zaid et al. (2023) described: the need for recovery-aware integrity frameworks that the literature had not yet supplied. The efficiency optimisation layer, for its part, held energy consumption low and latency acceptable across all test scenarios. Security and performance here function as complementary design variables, not competing ones, which is what Hussien et al. (2023) argued mobile cloud security models should achieve. Taken together, four integrated layers produced results that no single existing approach matched, and the second objective is validated accordingly.

6.0 CONCLUSION AND RECOMMENDATIONS

The central finding of this study is straightforward: information integrity in mobile cloud computing cannot be secured through single-layer mechanisms. Encryption, blockchain, and lightweight schemes each handle one part of the problem and leave the rest exposed, particularly around fault tolerance, recovery under network disruption, and security design that respects resource constraints. The proposed multi-level framework, integrating authentication, data validation, fault tolerance, and efficiency optimisation, returned an overall integrity rate of 96%, system reliability of 94%, and a latency of 1.8 seconds. It outperformed traditional encryption on integrity and blockchain-only systems on efficiency. These results provide empirical support for layered holistic security architectures in mobile cloud deployment.

Several recommendations follow from these findings. Organisations deploying mobile cloud systems should replace isolated mechanisms with integrated multi-level security frameworks. Fault tolerance and recovery must be treated as mandatory components of any integrity-assuring design, not optional additions to be considered after the fact. Security efficiency deserves treatment as a first-order design variable alongside protection strength, particularly where mobile and IoT devices operate under resource constraints. Cloud service providers should extend continuous data validation to the transaction level rather than limiting it to the point of storage. Future research should pursue real-world deployment evaluations to test whether simulation findings hold under practical conditions. Work is also needed on artificial intelligence integration for adaptive threat detection, on post-quantum cryptographic algorithms for future-resistant assurance, and on the scalability of frameworks of this kind in high-volume environments such as national mobile banking platforms and population-scale healthcare systems.

REFERENCES

Akbar, M., Waseem, M. M., Mehanoor, S. H., & Barmavatu, P. (2024). Blockchain-based cyber-



IJSGS FUGUSAU VOL. 12(3)	WEBSITE: https://fugus-ijsgs.com.ng
security trust model with multi-risk protection scheme for secure data transmission in cloud computing. <i>Cluster Computing</i>, 27, 9091-9105. https://doi.org/10.1007/s10586-024-04481-9 Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A review of security issues when integrating IoT with cloud computing and blockchain. <i>IEEE Access</i>, 12, 109560-109595. https://doi.org/10.1109/access.2024.3435845 Ali, S., & Al-Khalidi, M. (2024). Selective security and adaptive threat response in mobile cloud systems. <i>Journal of Computer Networks and Communications</i>, 2024, 1-14. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. <i>Journal of Computer Information Systems</i>, 66, 123-150. https://doi.org/10.1080/08874417.2024.2329985 Anderson, R. (2008). <i>Security engineering: A guide to building dependable distributed systems</i>. Wiley. Awadallah, R., & Samsudin, A. (2021). Blockchain-enhanced cloud architectures for mobile data protection. <i>Journal of Cloud Computing: Advances, Systems and Applications</i>, 10(1), 1-18. Awadallah, R., Samsudin, A., Teh, J., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. <i>IEEE Access</i>, 9, 69513-69526. https://doi.org/10.1109/access.2021.3077123 Chao, W. (2022). Distributed cloud security and mobile integrity assurance. <i>Journal of Cloud Systems</i>, 14(3), 201-218. Feng, L. (2022). Mobile cloud transaction vulnerabilities and security models. <i>International Journal of Information Security</i>, 21(4), 789-805. Feng, L., Zhang, Q., & Li, H. (2022). Multi-layer security frameworks for distributed mobile environments. <i>Computing and Security Review</i>, 9(1), 45-61. Goswami, P., Faujdar, N., Debnath, S., Khan, A. K., & Singh, G. (2024). Investigation on storage level data integrity strategies in cloud computing: Classification, security obstructions, challenges and vulnerability. <i>Journal of Cloud Computing</i>, 13. https://doi.org/10.1186/s13677-024-00605-z Hussien, Z., Abdulmalik, H., Hussain, M., Nyangaresi, V., Abduljabbar, Z., & Abduljaleel, I. (2023). Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems. <i>Applied Sciences</i>. https://doi.org/10.3390/app13020691 International Telecommunication Union. (2024). <i>Measuring digital development: Facts and figures 2024</i>. ITU Publications. Irshad, R. R., Hussain, S., Hussain, I., Nasir, J. A., Zeb, A., Alalayah, K., Alattab, A., Yousif, A., & Alwayle, I. (2023). IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing.	<i>IEEE Access</i>, 11, 105479-105498. https://doi.org/10.1109/access.2023.3318755 Kindervag, J. (2010). No more chewy centres: Introducing the Zero Trust Model. <i>Forrester Research</i>. Leila, M., Zitouni, A., & Djoudi, M. (2020). Ensuring user authentication and data integrity in multi-cloud environment. <i>Human-Centric Computing and Information Sciences</i>, 10, 1-20. https://doi.org/10.1186/s13673-020-00224-y Luo, F., Al-Kuwari, S., Lin, C., Wang, F., & Chen, K. (2022). Provable data possession schemes from standard lattices for cloud computing. <i>The Computer Journal</i>, 65(12), 3223-3239. Ming, Z. (2025). Lattice-based cryptographic integrity for mobile cloud environments. <i>Journal of Cybersecurity Research</i>, 18(2), 112-130. Ming, Z., Zhao, R., & Wu, S. (2025). Hybrid cryptographic models for mobile cloud data assurance. <i>Security and Communication Networks</i>, 2025, 1-17. Muhammad, A. (2024). Mobile cloud computing paradigms and emerging security challenges. <i>IEEE Transactions on Mobile Computing</i>, 23(5), 3401-3415. Muhammad, A., Khan, B., & Saleem, T. (2024). Transaction integrity in distributed mobile cloud systems. <i>International Journal of Cloud Computing</i>, 13(4), 289-308. Neoaz, N., & Amin, M. H. (2025). Ensuring information integrity in a mobile-connected world. <i>International Journal of Multidisciplinary Sciences and Arts</i>. https://doi.org/10.47709/ijmdsa.v3i4.5299 Neoaz, N., Bashir, A., & Rahman, K. (2025). Mobile cloud data protection models: A layered approach. <i>Journal of Information Assurance and Security</i>, 20(1), 33-50. Neoaz, N., Khatun, S., & Islam, R. (2025). Multi-factor trust verification in mobile cloud services. <i>International Journal of Advanced Networking and Applications</i>, 16(4), 6245-6258. Pfleeger, C. P., & Pfleeger, S. L. (2015). <i>Security in computing</i>. Pearson. Phatangare, S. (2024). Multi-level encryption system using AES and RSA algorithms. <i>International Journal for Research in Applied Science and Engineering Technology</i>. https://doi.org/10.22214/ijraset.2024.62420 Qayyum, R., & Ejaz, H. (2020). Data security in mobile cloud computing: A state of the art review. <i>International Journal of Modern Education and Computer Science</i>. https://doi.org/10.5815/ijmecs.2020.02.04 Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. <i>NIST Special Publication 800-207</i>. National Institute of Standards and Technology. Samydurai, A., Achuthan, R., Akash, K., & Eber Sheckel, E. (2023). Integrating multi-cloud to

IJSGS FUGUSAU VOL. 12(3)**WEBSITE: <https://fugus-ijsgs.com.ng>**

- establish cloud security for secured cloud transaction. *International Journal of Advanced Research in Science, Communication and Technology*. <https://doi.org/10.48175/ijarsct-8654>
- Shabbir, M., Shabbir, A., Iwendi, C., Javed, A., Rizwan, M., Herencsar, N., & Lin, J. C.-W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. *IEEE Access*, 9, 8820-8834. <https://doi.org/10.1109/access.2021.3049564>
- Shakor, M., Khaleel, M., Safran, M., Alfarhood, S., & Zhu, M. (2024). Dynamic AES encryption and blockchain key management: A novel solution for cloud data security. *IEEE Access*, 12, 26334-26343. <https://doi.org/10.1109/access.2024.3351119>
- Vallu, V. R., Pulakhandam, W., & Kurunthachalam, A. (2025). Revolutionizing mobile cloud security: Employing secure multi-party computation and blockchain innovations for e-commerce platforms. 2025 *International Conference on Artificial Intelligence and Emerging Technologies (ICAJET)*, 1-6. <https://doi.org/10.1109/icaiet65052.2025.11211015>
- Wang, C., Yuan, Z., Zhou, P., Xu, Z., Li, R., & Wu, D. O. (2023). The security and privacy of mobile-edge computing: An artificial intelligence perspective. *IEEE Internet of Things Journal*, 10, 22008-22032. <https://doi.org/10.1109/jiot.2023.3304318>
- Wang, L., Liu, J., & Zhao, H. (2023). Adaptive security protocols for mobile cloud transaction verification. *Journal of Network and Systems Management*, 31(3), 445-467.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security*. Cengage Learning.
- World Bank. (2025). World development indicators: Mobile cellular subscriptions. <https://data.worldbank.org/indicator/IT.CEL.SETS.P2>
- Wu, Y., Tan, X., & Xie, Q. (2024). Certificateless provable data possession scheme for cloud-based electronic health records system. *Mathematics*, 12(24), 3883.
- Yong, P. (2024). Information integrity lifecycle in mobile cloud healthcare environments. *Health Informatics Journal*, 30(1), 1-18.
- Yong, P., Cheng, F., & Xiao, M. (2024). Distributed integrity assurance models for sensor-driven cloud systems. *IEEE Sensors Journal*, 24(8), 14520-14534.
- Zaid, A. (2023). Fault-tolerant transaction frameworks for mobile cloud systems. *Journal of Parallel and Distributed Computing*, 178, 121-136.
- Zaid, A., Hamdan, O., & Farid, N. (2023). Lightweight recovery mechanisms for mobile cloud computing integrity. *Future Generation Computer Systems*, 145, 88-102.
- Zhao, M., & Chen, H. (2025). Identity-based provable data possession with designated verifier from lattices for cloud computing. *Entropy*, 27(7), 753.
- Zhao, R., & Lin, T. (2024). Provable data verification for real-time mobile transaction systems. *IEEE Transactions on Cloud Computing*, 12(2), 890-905.
- Zhou, C., Wang, L., & Wang, L. (2022). Lattice-based provable data possession in the standard model for cloud-based smart grid data management systems. *International Journal of Distributed Sensor Networks*, 18(4), 15501329221092940.
- Zhou, R., & Wang, Y. (2022). IoT-integrated mobile cloud systems and data integrity challenges. *Sensors*, 22(11), 4023.