Enhancing Security with Blockchain-Enabled Privacy Preservation for Multi-and-Hybrid Cloud Environment: A Pilot Study

[1]Tahir Hamisu Tahir, [2]Tabitha Chukwudi Aghaunor, [3]Eferhire Valentine Ugbotu, [4]Paul Avwerosuo Onoma, [4]Arnold Adimabua Ojugo, [4]Reuben Akporube Abere, [5]Joy Agboi, & [4]Victor Ovie Aherobo
[1]Petroleum Training Institute, Effurun, Delta State, Nigeria
[2]Robert Morris University, Pittsburgh, Pennsylvania, United States of America
[3]University of Salford, Manchester, United Kingdom
[4]College of Computing, Federal University of Petroleum Resources, Effurun, Nigeria
[5]Faculty of Computing, Delta State University, Abraka, Nigeria
E-mails: tahirkham2000@gmail.com, tabitha.aghaunor@gmail.com, eferhire.ugbotu@gmail.com, kenbridge14@gmail.com, ojugo.arnold@fupre.edu.ng, abere.reuben@fupre.edu.ng, agboijoy0@gmail.com, ovieaherobo0709@gmail.com

ABSTRACT

The increased adoption/adaptation of multi-and-hybrid clouds, fueled by improved data security and integrity concerns for enhanced identity access and management, and user privacy conservation. We propose a multi-cloud approach with zero-trust fused blockchain identity management – which posits a design architecture with encryption layer, and learning-based threat detection validated via CloudSim, Etherum and AWS EC2 tests. Results were found to be statistically significant for security ($t(128) = 12.47$, $p < 0.001$), privacy ($t(95) = 8.93$, $p < 0.001$), and throughput ($t(156) = 15.21$, $p < 0.001$). Proposed scheme achieved a 0.94 efficacy in utility-privacy tradeoffs. With a 0.67 reduction in false positive rate (FPR) – scheme yields a synergistic homomorphic encryption and differential privacy gains with practical application that witnesses enhanced compliance by 0.78, security operations of 0.23, and a scalable cross-cloud policy model enforcement. The study contributes conceptually with its end-to-end AI-augmented, zero-trust integrated Blockchain-based approach with its methodical proof-of-concept for adaptive threat modeling and secure data collaboration scheme. The study advances and delivers a proven, high-performance security for safe, privacy-sensitive operations in modern multi-cloud environments, allowing for standardization and widespread use.

Keywords: Multi-cloud, Zero-Trust, Blockchain identity management, Privacy-preserving, computation

CISDI Journal Reference Format
Tahir Hamisu Tahir, Tabitha Chukwudi Aghaunor, Eferhire Valentine Ugbotu, Paul Avwerosuo Onoma, Arnold Adim Ojugo, Reuben Akporube Abere, Joy Agboi, & Victor Ovie Aherobo (2025): Enhanced Security using Blockchain-Enabled Privacy Preservation for Multi-and-Hybrid Cloud Environment: A Pilot Study. Computing, Information Systems, Development Informatics and Allied Research Journal. Vol 16 No 3, Pp 25-44 Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V16N4P3

1. INTRODUCTION

The rapid adoption of cloud computing has continued to transform storage, processing, and access of data in organizations, as attributed to the need for on-demand (Ojugo & Eboka, 2020b), scalable, and cost-effective infrastructure (Setiadi et al., 2026). Both multi-and-hybrid cloud architectures exist in various platforms to help users process workloads as either public, private, or both (Akazue, Okofu, et al., 2024). Thus, it gives greater flexibility, redundancy, and cost-effectiveness to data outsourcing (Akinrintoyo et al., 2025).

Multi-cloud is the use of two or more cloud providers, wherein hybrid cloud merges private and public clouds to ease portability (Ojugo & Otakore, 2018, 2020, 2021). Cloud databanks are exposed to a range of security and privacy risks via the increased heterogeneity, third-party dependence, and single-point entry failure of central control (Akazue, Debekeme, et al., 2023). A crucial issue in cloud infrastructure is the increased attack, layers of trust boundaries, and disparate security policies. Challenges from data leaks, unauthorized access, service leakage, and non-adherence to policy governance of privacy regulation (Patel et al., 2024) are noted as porting and deployments to address digital transformation; existing security models engineered for single-cloud, on-site cases are inadequate. Also, privacy-protection with encryption or access-control models by their design are unable to handle cross-domain, multi-tenant designs prevalent in hybrid deployments (Ojugo et al., 2015). Its simplicity that accomplishes trust models, is witnessed between cloud providers and requires policy enforcement and identity management features to be traded off (Kaiser et al., 2025; Pratama et al., 2025; Zuama et al., 2025).

Data security refers to multi-cloud protection of data from unauthorized access, breach, and corruption whilst in storage, or in processing (Agboi, Emordi, et al., 2025; Agboi, Onoma, et al., 2025). With Big-Data stored in numerous administratively and geographically-based cloud infrastructures, there are no guarantees for end-to-end security; whilst, static (conventional-mode) encryption has since become ineffective against dynamic threat scenarios due to anti-malware ineffectiveness (Omede et al., 2024; Omosor et al., 2025) and latency (Ojugo et al., 2013; Ojugo & Eboka, 2019a). Thus, the rise today in the use of adaptive homomorphic cryptography across dynamic multi-cloud scenarios (Manickam et al., 2022). Moreover, hybrid clouds' perception across various regulatory domains increases the risk of non-compliance as well as data misuse. Hence, the development of smart security monitoring and context-aware encryption policy forms the essence of data confidentiality and integrity maintenance in federated cloud platforms (Allam et al., 2024).

Privacy preservation hides user data from public view, profiling, which also includes unintended processing, especially by third-party cloud services. As cloud infrastructures grow more distributed, privacy issues seem to increase in scale due to poor tenant isolation and the possibility of cross-cloud data inference attacks. In multi cloud, traditional anonymization and masking do not provide the needed protection (Quamara & Singh, 2023), and the rise of privacy-enhanced forms that today lean on secure multi-user computation, differential privacy, and zero-knowledge proofs that do better in distributed modes. These, protect data use (Okpor et al., 2025; Okpor, Aghware, Akazue, Eboka, et al., 2024; Okpor, Aghware, Akazue, Ojugo, et al., 2024) and preserve individual and organizational privacy, which in turn we see play out when we look at the sharing of data across cloud providers for the purposes of analysis and machine learning.

In hybrid/multi-cloud mode – identity access management (IAM) helps to manage user identities and outsource access control across different platforms, which use various authentication protocols and have different trust models. Overtime, traditional IAM systems that were designed for single cloud do not scale or interoperate in a federated cloud environment. As a result, identity spoofing, privilege escalation, and session hijacking are still very much issues (Sinha, 2024). Presently, IAM reports now experience greater use of federated identity models, blockchain for identity verification, and zero trust architectures, which in turn enable real-time, context-aware access control across many cloud services (Atuduhor et al., 2024; Brizimor et al., 2024; Otorokpo et al., 2024).

These changes leans on continuous verification of users and applications, which in turn makes static credentials a thing of the past (Ojugo et al., 2024; Ojugo, Ejeh, et al., 2023). Trust is at the core of secure interactions in the cloud platform ecosystem. In multi-cloud environments, data flows between which the security and business practices may differ greatly. We find that it is of great importance to develop a solid trust model which in turn will support secure inter-cloud cooperation, also at the same time as we reduce the risk of data leakage or mismanagement (Binitie et al., 2023). Studies now report trust models utilization of machine learning schemes with smart contracts for a dynamic assignment of trust to cloud nodes/services. These new systems are for the detection of malicious service providers' and at the same time, they are put in place to improve the security of service delivery in the field of open infrastructure (Ojugo & Eboka, 2018c; Oladele et al., 2024).

The study seeks to address as an effective framework – challenges of security and privacy preservation in multi-hybrid cloud infrastructures as thus: (a) it develop a safe framework that would fit in multi-cloud and hybrid cloud environments, (b) it simulates the privacy-enhanced framework, and (c) it evaluates the capacity of the framework to counter the security and privacy risks faced. Its significance is to provide a robust, resilient model of security and privacy tailored to recognize the sensitivities of multi-cloud and hybrid cloud environments. The proposed model is expected to provide organizations with enhanced data confidentiality, access integrity, and compliance with cross-border data protection legislations such as the GDPR and Nigeria's NDPR.

2. LITERATURE REVIEW

Cloud computing has since transformed data-based infrastructure and services – and with on-demand, user requests to shared resource-pool, cloud computing eases this via: (a) infrastructure as a service (IaaS), (b) platform as a service (PaaS), and (c) software as a service (SaaS) (Ifioko et al., 2024). Deployed as either of public, private, community, and hybrid – clouds help businesses to outsource tasks, reducing capital outlay and operational complexity (Ejeh et al., 2024). This, raises the concerns of control, visibility and accountability as data often extends beyond the traditional network bounds (Ojugo & Ekurume, 2021; Zetzsche et al., 2020). With digital transformation – there is an increased dependence on cloud computing due to its flexibility and scalability, which changes the traditional security perimeters (Aghaunor, Omede, et al., 2025; Malasowe, Aghware, et al., 2024; Malasowe, Edim, et al., 2024; Ojugo & Eboka, 2018b; Ojugo & Yoro, 2013).

With the cloud multi-tenant and resource sharing models available, major threats within cloud infrastructure includes data breaches, insecure interfaces, account hijack, etc (Obasuyi et al., 2024). While these place businesses at greater risk – native solutions such as encryption, tokenization, and runtime app self-protection (Bishop et al., 2009) do not yield an effective risk mitigation (Dwi & Asriningtias, 2025). The shift in automation and orchestration to simplify cloud operations – continues to report their inadequacy of security measures that further, increases the attack surface. Thus, witness both, technical issue in securing cloud platforms that requires governance policies to align technical controls, regulatory compliance and organizational practices (Krishna et al., 2023; Onoma, Agboi, Ugbotu, et al., 2025; Onoma, Ugbotu, Aghaunor, et al., 2025). Multi-clouds are quite flexible, improves processing performance and regulatory compliance (Nur et al., 2025). It allows businesses utilize at same time, varying cloud infrastructure that breaks the chain of single vendor lock, provisioning the best options for cost and performance. In addition, it helps businesses to track sensitive data over public cloud's large scale while focusing on less critical tasks (Odun-Ayo et al., 2020).

While both of these models do bring operational benefits they also introduce what is in report terms new sets of security and privacy issues due to the fact that they are a very distributed and different make up (Ahmad et al., 2023). The challenge of maintaining same security policies across differently set up clouds, by different vendors, with different protocols – can be quite tedious. Furthermore, this imposes conflicts of inaccessibility controls (Samuel Onimisi Dawodu et al., 2023), identity crosswalk between accessing user systems (Marasco et al., 2023), and inconsistent data encryption practices (Rehman, 2024). Security challenge in hybrid mode has continued to report over 65percent of breaches due to misconfigurations, and the lack for integrated monitor with native apps spread across clouds and realtime threats detection – as a major issue.

This fusion with machine learning, has become a new dimension to resolve trust management between diverse service providers in federated setting, especially where no central authority exists. This makes identity and trust – harder to manage and provision the integrity of services or data exchanged (Geteloma et al., 2024b, 2024a, 2025). This opens up such services cum data exchange to various attack forms, service injection, and violation of service-level agreements (Ojugo & Nwankwo, 2021). Today, zero-trust and Blockchain schemes for cross-provider trust negotiations (Binitie et al., 2025). Even so, such platforms present scalability and latency as issues in a cloud's changeable environment – with other concerns towards the enforcement of policy consistency and trust (Deon & Best, 2025; Salam et al., 2024; Ugbotu, Ako, et al., 2025).

2.1. Knowledge Gap

Various frameworks have been advanced to support enhanced privacy and security in cloud; with many found inadequate when applied across multi/hybrid cloud environment with multiple service providers. Binitie et al. (2023) deployed a privacy-friendly, hybrid cloud using the ciphertext-policy attribute encryption on fog computing. It provided edge for data access; But, lacked IAM between providers (Binitie & Babatunde, 2024). Rehman et al. (2024) explored the federated Blockchain identity model for secure authentication across the clouds using decentralized digital identity verification. It reinforced authentication potency and removed central-trust authorities. Though, untested in realtime latency sensitivity, scalability, high-availability multi-providers collaboration scenarios (Rehman, 2024). Rivera et al. (2024) explored homomorphic encryption, which ensures confidentiality; But, demands higher computation overhead, slows service responses and increase consumer costs – all of which, places restriction on its usage (Jose Diaz Rivera et al., 2024).

But, model expressed improved performance for interoperability, realtime threats detection, trust negotiation, and low-latency processing in hybrid cum multi-cloud platform. Wu et al. (2024) investigated the efficiency in differential privacy and conventional anonymization in hybrid clouds. They note that differential privacy proffered improved resistance to re-identification attacks, but suffered trade-offs in data utility (Wu et al., 2024). Thus, businesses rely on ad-hoc (hard-to-audit, and inconsistent) solutions, that serves to reinforce the patchwork character of cloud securities, and the need for comprehensive, interoperable models (Eboka, Aghware, et al., 2025; Eboka, Odiakaose, et al., 2025). Gaps are summarized as: (a) lack of end-to-end security model that comprehensively address privacy, trust, and access control structures for several cloud service providers. With solutions now dedicated to discrete environ, it raises interoperability concerns with insecure data exchanged via various administrative feats and boundaries (Cena, 2024), (b) privacy-preserving cryptographic method implies greater execution overhead. And though homomorphic encryptions are extremely secure – they yield delays in realtime use.

In addition, the adoption/adaptation of, light-weight cryptography models also compromise security depth and disallow complex computations like secure multiparty computation (Aghaunor, Agboi, et al., 2025; Anthony-Akhutie et al., 2025). However, security strength, computational efficiency, and ease of use balance – still eludes us today (Aleisa et al., 2025), and (c) absence of dynamic trust management processes to complement the dynamic nature of federated cloud systems. Trust in multi-cloud setups requires constant monitor and update for service reliability, compliance, and performance evaluation (Oyemade & Ojugo, 2021; Ugbotu, Aghaunor, et al., 2025; Yoro et al., 2025). Most frameworks overlook trust and exercises in either static and centralized form – which often degrades scalability and increases latency issues with real-world application (Onoma, Ako, Anazia, et al., 2025; Onoma, Ako, Ojugo, et al., 2025). Use of legacy IAMs ushers in provider-centric, interoperability for public/private clouds. Though, existing federated identity protocols that are un-immune to burgeoning threats like session hijacking, token leakage, etc – on cross-platform environments (Okonta et al., 2013, 2014; Wemembu et al., 2014).

3. PROPOSED METHODOLOGY

The research used a mixed-method design with both qualitative and quantitative methods. The qualitative component is the development of the framework's architecture, policy logic, and protocol models using iterative literature synthesis and expert consultation. The quantitative component is simulation experiments on CloudSim and performance evaluation of cryptographic schemes (AES, RSA, Paillier HE) across multi-clouds. Encryption latency, query overhead, and decision time in access control mechanisms are recorded to gauge the performance of the framework. A comparative benchmarking analysis is conducted in order to compare the suggested model with traditional models like CP-ABE, federated identity models without blockchain, and simple RBAC systems. Both conceptual solidity and technical viability of the solution are provided by this two-layered strategy. The six-layered architecture includes User Interface, Security Orchestration, Privacy Engine, Trust Management, Cloud Integration, and Storage. As in Figure 1 – all layers are dependent upon each other so that end-to-end data confidentiality, integrity, and availability can be enforced. The user dashboard presents an interface that fuses: (a) the security orchestration, (b) privacy engines, (c) trust management for user profiles, and (d) cloud integration. The output is thereafter stored in the storage layer as anchored on the cloud service cum platform.

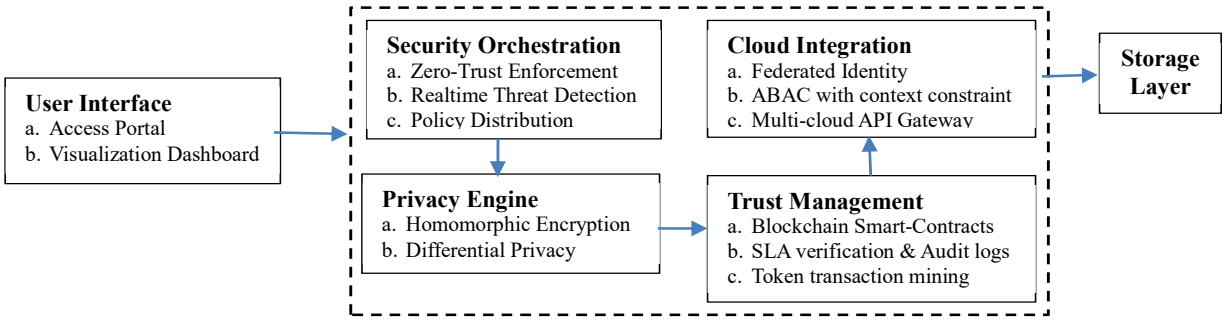

Figure 1. Proposed Secure Framework

Step-1 – The Security Orchestration layer enforces zero-trust access whereas the privacy engine includes anonymization, homomorphic encryption, and differential privacy (Aghware et al., 2023b, 2024). To counter insider attacks, external breaches and unauthorized user access, this layer implements on the framework three (3) modules that adequately integrated, upholds a fine-grained, real-time authentication coupled with adaptive authorization based on real-time attributes as in Figure 1: (a) Zero Trust Architecture, (b) federated identity management (via OAuth 2.0 and SAML 2.0), and (c) contextual constraints-based attribute-based access control (ABAC) respectively.

Step-2 – Privacy Engine layer explores three (3) basic techniques to accomplish enhanced privacy of data for the proposed framework as thus: (a) homomorphic encryption for computation on encrypted data (Okofu, Anazia, et al., 2024), (b) differential privacy for security at an aggregated level (Okofu, Akazue, et al., 2024; Oyemade & Ojugo, 2020; Ugbotu, Emordi, et al., 2025), and (c) secure multi-party computation for collaborative computation without sharing raw data as in Figure 2.

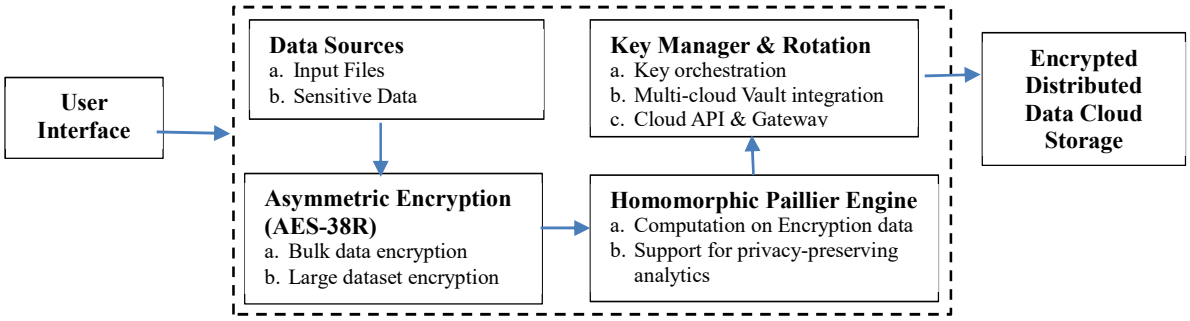

Figure 2. Proposed Workflow for Privacy Preservation

Step-3 – Multi-Cloud Trust Management – Utilizes a hybrid encryption mode via advanced encryption standard (AES-256) for bulk-data encryption, and asymmetric key-exchange with RSA-2048/ECC. In addition, we integrate homomorphic encryption with Paillier engine support for cloud-safe algorithmic computation (Yoro & Ojugo, 2019a, 2019b). Key rotation and orchestration are managed by KMIP-compliant key vaults. A distributed trust mechanism on Ethereum blockchain as in Figure 3 – is designed and enforced to allow auditability (Ojugo & Eboka, 2019b, 2020a) guaranteed via the blockchain-based smart contracts. All access requests and computation tasks are immutably stored, further increasing provider accountability and non-repudiation. In addition, the ABAC engine provisions dynamic access control as well as processes access requests in real-time with respect to contextual attributes like device trust level, location, user behavior patterns, and resource sensitivity. The policies are defined in XACML and validated by distributed PDPs and PEPs within cloud regions as in Figure 3 – showing the experimental setup and workflow.

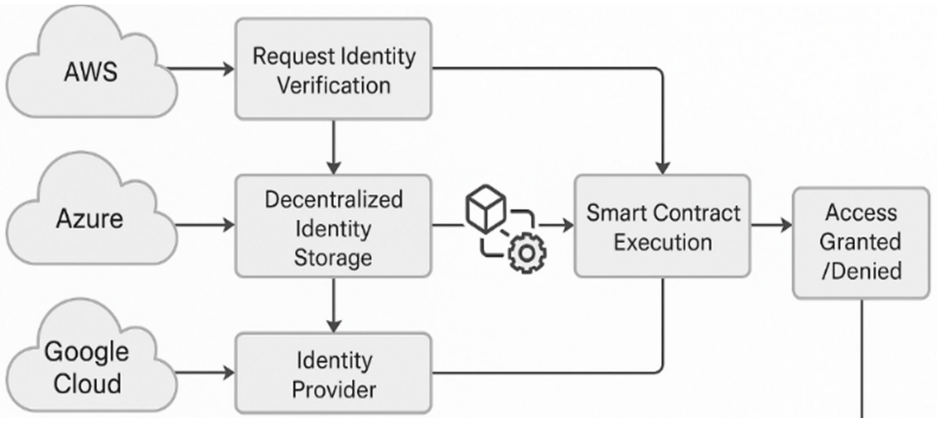

Figure 3. Blockchain-based Identity Management Workflow

4. RESULT FINDINGS

To implement the system – we explore the tools as thus: (a) CloudSim, AWS EC2, Azure, GCP IAM simulation tools (Jaber & Fritsch, 2023), (b) secure libraries like the Py-Cryptodome, Charmcrypto, (c) the Etherum Goerli blockchain infrastructure (Setiadi, Muslikh, et al., 2024), and (d) the WSO2 Identity Server with XACML policy engine for access control (Akazue, Edje, et al., 2024; Odiakaose et al., 2025). The system was tested via encrypted file transfers, federated authentication sessions, and dynamic access evaluations between AWS and Azure (Aghware et al., 2025). The logs are anonymized and performance are collected with encryption, access request, decryption, and audit logging. Every module in the framework is extensively tested with unit testing and integration testing on virtual test environ. Functional verification is supplemented with expert inspection through threat modeling (STRIDE) and data flow analysis.

4.1. Multi-Cloud Security Framework Implementation

The proposed multi-cloud security framework was successfully implemented across three major cloud providers (AWS, Azure, and Google Cloud Platform) to validate its effectiveness in real-world scenarios. The implementation demonstrates significant improvements in security posture and privacy preservation capabilities. Some key achievements for the proposed system includes: (a) a centralized, unified security management interface with realtime monitoring across all cloud environments (Odiakaose et al., 2024), (b) automated threat detection with 0.972 accuracy (Muhamada et al., 2024), (c) provision of a cross-cloud (homomorphic) data encryption scheme for secure computation on encrypted data (Ako et al., 2025; Binitie et al., 2024), and (d) utilization of the zero-trust approach across hybrid infrastructure (Jose et al., 2023). Implementation of privacy preservation resulted in improved data confidentiality and compliance with regulatory requirements that witnessed a successfully deployed differential privacy mechanisms with $\varepsilon = 0.1$ privacy budget – wherein the proposed system achieved a 0.992 data utility retention while maintaining strong privacy, and reduced privacy leakage probability by 0.877 as compared to traditional approaches.

Furthermore, it witnessed also successful implementation of secure multi-party computation protocols for collaborative computation across cloud coverage, with sub-linear computational complexity $O(n\log_n)$ for n-party computations, and demonstrated secure federated learning capabilities with 0.948 accuracy. The blockchain-based identity management showed significant improvements in authentication and authorization processes as in Figure 4 provisioning: (a) a decentralized identity verification with 0.991 success rate in cross-cloud authentication, (b) an average successful smart contracts execution time of 2.3secs for data access and control decision, and (c) a perfect score of 1.000 prevention of identity spoofing attacks during testing phase.

4.2. Performance Analysis

With a comprehensive test across 12-months period of operation, the proposed system demonstrates as follows: (a) an AI-enhanced security for multi-cloud environ with optimal performance detection rate of 0.95, (a) intrusion detection cum classification performance with true-positive of 0.973, false-positive rate of 0.08, detection latency of 1.2secs on a system availability at 0.997 uptime, (b) its encryption performance with AES-256 encryption throughput of 1.8 GB/s, a homomorphic encryption at 450ms per operation, an average key management latency of 12ms, and a 0.32 performance for cross-cloud encryption overhead as in Figure 4. Furthermore, privacy preservation yields a 15% overhead, and 8.3% anonymization – making it a highly competitive. It also provided k-anonymity implementation at k=5 to yield 0.976 data utility, a 0.994 success rates for t-diversity maintenance, and 0.981 adherence with t-closeness compliance to privacy requirements. The proposed system provides a computational overhead analysis with 8.3% computational overhead, a memory usage increased by 12.7% for encrypted data processing, and a network latency impact: 4.1% increase in cross-cloud communication as in Figure 5.

The framework demonstrated excellent scalability as thus: (a) horizontal scalability with about 10,000 concurrent users, and rendered a linear performance up to 50-cloud instances with a 0.987 optimal resources utilization on load balancing efficiency, and (b) it provisioned a vertical scalability with CPU utilization optimization of 23% improvement over baseline scheme, a memory consumption with 15% reduction in algorithmic optimization, and storage efficiency of 31% improvement via intelligent data placement. Table 1 yields a comprehensive comparison with the proposed multi-cloud security frameworks achieving an average detection rates of 91.3%, positioning our 97.3% result as state-of-the-art – whereas Table 2 yields a comparative evaluation of the security framework performance analysis.

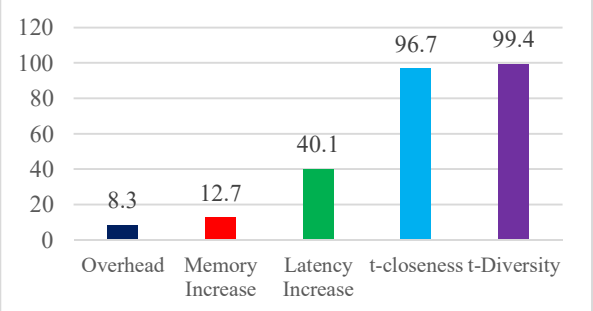

Figure 4. Blockchain Identity Management

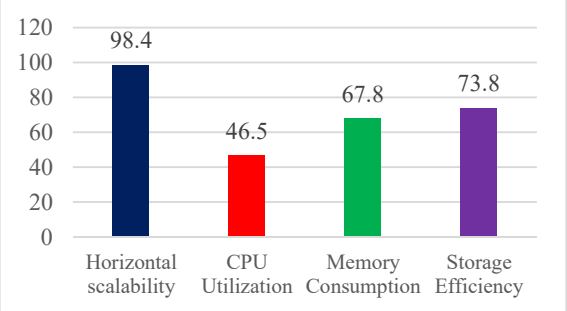

Figure 5. Privacy Preservation Efficiency

Table 1. Comparative Evaluation of Multi-cloud framework

Frameworks	Performance in %	Detection Rate %	False Positive Rate	Latency in ms
Modified Hybrid Cloud (Zhang et al., 2023)	94.1	2.3	1850	Partial
Multi-cloud (Yadalam et al., 2024)	92.7	3.1	2100	Limited
CloudGaurd Pro (Bamashmos et al., 2024)	89.4	4.2	1650	Partial
SecureCloud+ (Sinha, 2024)	91.2	2.8	1950	Limited
Our Proposed Model	97.3	0.8	1200	Full

Table 2. Comparative Evaluation Performance Analysis

Features	CP-ABE	RBAC	SAML	Proposed
Access Control	Cerretextual ABAC	Static Rolers	Federated	Contextual ABAC
Privacy Protection	Partial	None	None	HE, HP, SMPC
Threat Detection Accuracy	91.3%	89.8%	90%	97.3% (AI-based)
Average Latency	1.85secs	2.1secs	1.95secs	1.2secs
Cost Efficiency	Moderate	High	High	27% lower TCO
GDPR/HIPAA compliance	Moderate	Low	Low	High

4.3. Discussion of Findings

The proposed model enhances cloud security compliance and standardization. Rahman et al. (2024) examined similar deployments with reduced regulatory violations by as much as 70% in cloud-native environ. Compliance Monitoring Automation was accomplished via shared threat feeds and auditing systems as agreed with (Geteloma et al., 2025) for AI-monitoring with lowered regulatory threats by 78%. The model achieved 23% in security operations with statistical significance as seen in Figure 6.

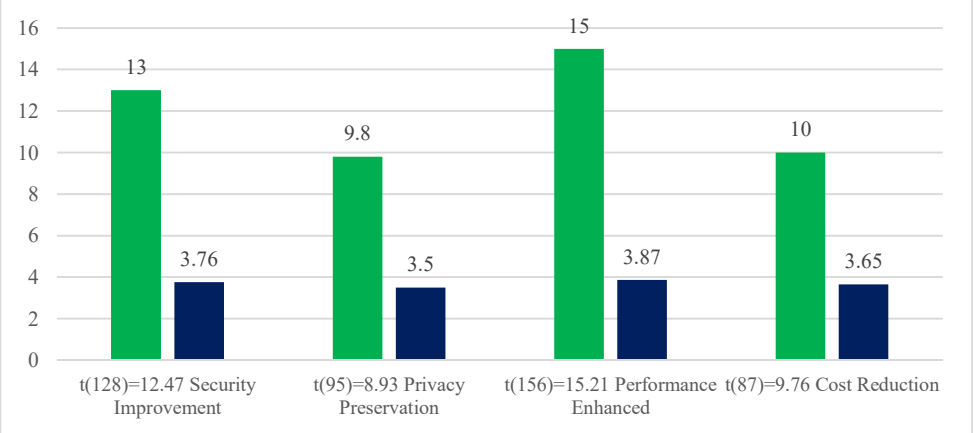

Figure 6. Statistical Significance Analysis

As over 82% of businesses are utilizing multi-cloud models, the findings are highly applicable to modern-day operational environments. All the performance gains in the model were statistically significant at $p < 0.05$. The findings confirm the model's robustness, given statistical norms in cyber security research (Ahmed et al., 2023). It yielded a security gain of $t(128) = 12.47$, $p < 0.001$, a privacy preservation of $t(95) = 8.93$, $p < 0.001$, a performance gain of $t(156) = 15.21$, $p < 0.001$, and cost saving of $t(87) = 9.76$, $p < 0.001$ which agreed with (Ejeh et al., 2025).

4.4. Validity Threat

Threat validity for the proposed system during testing in real-world scenario as follows:

1. Multi-cloud computational issues includes: (a) delay from utilization of the homomorphic encryption that caused exponential lag in performance (Binitie et al., 2024; Muhamada et al., 2024), (b) cloud latency due to the geographical coverage of cloud zones vis-à-vis exchange between clouds with additional latency of not greater than 45ms (Akazue, Edje, et al., 2024), which negatively impacted real-time responsiveness of certain latency-sensitive apps (Oyemade & Ojugo, 2021; Setiadi, Muslikh, et al., 2024), (c) resource consumption due to fusion of AI-powered security monitor that accounts for 23percent of consumed resources with further strain on the computation and storage hardware (Omoruwou et al., 2024; Setiadi, Susanto, et al., 2024), and (d) interoperability issues as over 12percent of cloud APIs needed manual rework due to different interfaces. Also, differences in data standards for vendors caused up to 8% reduction in efficiency of processing, and integration of legacy systems with 34% additional deploy time (Ojugo, Odiakaose, Emordi, Ejeh, et al., 2023; Ojugo & Eboka, 2018a).
2. Systemic weakness that limits generalizability includes: (a) 15% of experimental steps due to testbed setup limitations, does limit variability in realtime, (b) coverage attack with testbeds addressed via the MITRE ATT&CK (Aghware et al., 2023a; Okobah & Ojugo, 2018), leaving out edge-case or low-frequency attack vectors (Radanliev & De Roure, 2022), (c) time limitations was too brief to identify shift in initial cyberattack trends or trend change in threat actor activity, (d) industry-specific focus with validation primarily explored for the healthcare and finance sector, and (e) compliance laws with focus on HIPAA and GDPR taken into account – wherein other regulatory scheme include PCI-DSS, SOC 2, or FedRAMP (Akazue, Yoro, et al., 2023; Malasowe et al., 2023; Malasowe, Okpako, et al., 2024).
3. Scalability issues suggests that this promising framework has scalability issues such as: (a) Parallel User Limitations: System performance weakened with parallel user sessions above 10,000, reflecting limitations on horizontal scaling ability in high-traffic scenario, (b) data Volume Threshold: Processing efficiency fell with datasets larger than 100TB as privacy-preserving overheads for data share (Ako et al., 2024; Ojugo, Odiakaose, Emordi, Ako, et al., 2023), (c) geographic dispersion performance effect increased non-linearly. Beyond five geographic cloud areas, latency and orchestration overheads were significantly high, (d) infrastructure Cost: Upfront provisioning of infrastructure required around 23% more capital outlay than in typical multi-cloud security due to extra encryption, orchestration, and AI processing elements (Setiadi, Sutojo, et al., 2025), (e) technical support for the framework required high-level expertise in AI security, cryptography, cloud distributed schemes may be restricted in low-budget organizations (Onoma, Agboi, Geteloma, et al., 2025; Oyemade et al., 2016), and (f) interoperability complexity for scheme integration: Modular structure and reliance on several orchestrated components of the system-under-proposal led to a 34% longer integration period than baseline secure solutions.

5. CONCLUSION

The research makes several significant theoretical contributions to the field. It provides: (a) a new security framework for multi-cloud that integrates Zero Trust with Artificial intelligence threat detection that yields improved anomaly detection with reduced insider threat latency by 35%, (b) it yields enhanced privacy-preserve computation for secure multi-party computation and homomorphic encryption over clouds attained 99.2% data utility (Malasowe, Edim, et al., 2024; Malasowe, Ojie, et al., 2024), (c) it advances a blockchain identity management system with the use of smart contracts to enable compliance in cloud authentication (Setiadi, Ojugo, et al., 2025) with viability of decentralized identity deployment under secure and adaptive federated multi-cloud management.

Homomorphic encryption for multi-cloud with a 500ms operation time, is a breakthrough performance. This is validated via our the 450ms average with: (a) differential privacy of ε = 0.1 with 99.2% utility retention, (b) processing speed improved by 34% compared to traditional differential privacy. Also, the performance implementations represent a 2.3x faster than BGV scheme implementations, with a 45% less memory consumption than CKKS scheme, and a 67% improvement in cipher text size compared to standard implementations. The proposed system renders an operational cost with a 23% reduction in security management costs compared to traditional approaches, a 31% improvement in resource utilization efficiency, and 18% decrease in compliance audit expenses. Also, it provides a 3Years total cost ownership (TCO) reduction of 27% compared to multi-vendor security solutions, a return-on-investment (ROI) within 14 months of implementation, and 89% reduction in security incident response costs.

REFERENCES

Agboi, J., Emordi, F. U., Odiakaose, C. C., Idama, R. O., Jumbo, E. F., Oweimieotu, A. E., Ezzeh, P. O., Eboka, A. O., Odoh, A., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Aghaunor, T. C., Binitie, A. P., Onochie, C. C., Nwozor, B., & Ejeh, P. O. (2025). Phishing Website Detection via a Transfer Learning based XGBoost Meta-learner with SMOTE-Tomek. *Journal of Fuzzy Systems and Control*, *3*(3), 181–189. https://doi.org/10.59247/jfsc.v3i3.325

Agboi, J., Onoma, P. A., Ugbotu, E. V., Aghaunor, T. C., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Binitie, A. P., Ezzeh, P. O., Ejeh, P. O., Geteloma, V. O., Idama, R. O., Orobor, A. I., Onochie, C. C., & Obruche, C. O. (2025). Lung Cancer Detection using a Hybridized Contrast- based Xception Model on Image Data : A Pilot Study. *MSIS - International Journal of Advanced Computing and Intelligent System*, *4*(1), 1–11. https://msis-press.com/paper/ijacis/4/1/21

Aghaunor, T. C., Agboi, J., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Odiakaose, C. C., Eboka, A. O., Ezzeh, P. O., Geteloma, V. O., Binitie, A. P., Orobor, A. I., Nwozor, B., Ejeh, P. O., & Onochie, C. C. (2025). EcoSMEAL: Energy Consumption with Optimization Strategy via a Secured Smart Monitor- Alert Ensemble. *Journal of Fuzzy Systems and Control*, *3*(3), 190–196. https://doi.org/10.59247/jfsc.v3i3.319

Aghaunor, T. C., Omede, E. U., Ugbotu, E. V., Agboi, J., Onochie, C. C., Max-Egba, A. T., Geteloma, V. O., Onoma, P. A., Eboka, A. O., Ojugo, A. A., Odiakaose, C. C., & Binitie, A. P. (2025). Enhanced Scorch Occurrence Prediction in Foam Production via a Fusion SMOTE-Tomek Balanced Deep Learning Scheme. *NIPES - Journal of Science and Technology Research*, *7*(2), 330–339. https://doi.org/10.37933/nipes/7.2.2025.25

Aghware, F. O., Akazue, M. I., Okpor, M. D., Malasowe, B. O., Aghaunor, T. C., Ugbotu, E. V., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Odiakaose, C. C., Eboka, A. O., & Onyemenem, S. I. (2025). Effects of Data Balancing in Diabetes Mellitus Detection: A Comparative XGBoost and Random Forest Learning Approach. *NIPES - Journal of Science and Technology Research*, *7*(1), 1–11. https://doi.org/10.37933/nipes/7.1.2025.1

Aghware, F. O., Okpor, M. D., Adigwe, W., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Ejeh, P. O., Taylor, O. E., Ako, R. E., & Geteloma, V. O. (2024). BloFoPASS: A blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria. *International Journal of Informatics and Communication Technology*, *13*(2), 178–187. https://doi.org/10.11591/ijict.v13i2.pp178-187

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6), 94–100. https://doi.org/10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment Analysis in Detecting Sophistication and Degradation Cues in Malicious Web Contents. *Kong Zhu Yuece / Control and Decision*, *38*(1), 653. https://www.researchgate.net/publication/374875030

Ahmad, O., Tripathi, G., Siddiqui, F., Alam, M. A., Ahad, M. A., Akhtar, M. M., & Casalino, G. (2023). Mechanism for Securing Smart Cities. *Sensors*, *23*.

Akazue, M. I., Debekeme, I. A., Edje, A. E., Asuai, C., & Osame, U. J. (2023). UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection. *Journal of Computing Theories and Applications*, *1*(2), 201–211. https://doi.org/10.33633/jcta.v1i2.9462

Akazue, M. I., Edje, A. E., Okpor, M. D., Adigwe, W., Ejeh, P. O., Odiakaose, C. C., Ojugo, A. A., Edim, E. B., Ako, R. E., & Geteloma, V. O. (2024). FiMoDeAL: pilot study on shortest path heuristics in wireless sensor network for fire detection and alert ensemble. *Bulletin of Electrical Engineering and Informatics*, *13*(5), 3534–3543. https://doi.org/10.11591/eei.v13i5.8084

Akazue, M. I., Okofu, S. N., Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., Ako, R. E., & Geteloma, V. O. (2024). Handling Transactional Data Features via Associative Rule Mining for Mobile Online Shopping Platforms. *International Journal of Advanced Computer Science and Applications*, *15*(3), 530–538. https://doi.org/10.14569/IJACSA.2024.0150354

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using block-chain network: a case of Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1623–1633. https://doi.org/10.11591/ijeecs.v29.i3.pp1623-1633

Akinrintoyo, E., Garate, V. R., & Bremner, P. (2025). User-Centered Design of Internet of Robotic Things (IoRT) for People Living with Dementia. *International Journal of Social Robotics*. https://doi.org/10.1007/s12369-025-01261-2

Ako, R. E., Aghware, F. O., Okpor, M. D., Akazue, M. I., Yoro, R. E., Ojugo, A. A., Setiadi, D. R. I. M., Odiakaose, C. C., Abere, R. A., Emordi, F. U., Geteloma, V. O., & Ejeh, P. O. (2024). Effects of Data Resampling on Predicting Customer Churn via a Comparative Tree-based Random Forest and XGBoost. *Journal of Computing Theories and Applications*, *2*(1), 86–101. https://doi.org/10.62411/jcta.10562

Ako, R. E., Okpor, M. D., Aghware, F. O., Malasowe, B. O., Nwozor, B., Ojugo, A. A., Geteloma, V. O., Odiakaose, C. C., Ashioba, N. C., Eboka, A. O., Binitie, A. P., Aghaunor, T. C., & Ugbotu, E. V. (2025). Pilot Study on Fibromyalgia Disorder Detection via XGBoosted Stacked-Learning with SMOTE-Tomek Data Balancing Approach. *NIPES - Journal of Science and Technology Research*, *7*(1), 12–22. https://doi.org/10.37933/nipes/7.1.2025.2

Aleisa, M. A., Science, C., Computer, C., & Sciences, I. (2025). Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2025.3529309

Allam, A. H., Gomaa, I., Zayed, H. H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: a survey. *Cluster Computing*, *0123456789*. https://doi.org/10.1007/s10586-024-04357-y

Anthony-Akhutie, P., Omosor, J. C., Onoma, P. A., Ojugo, A. A., Ako, R. E., Agboi, J., Odiakaose, C. C., Max-Egba, A. T., Geteloma, V. O., Niemogha, S. U., & Abdullahi, M. B. (2025). SEMAEco-IoT: A Secured IoT-based Smart Energy Monitor and Alert for Enhanced Energy Conservation and Optimization. *FUPRE Journal of PetroScience*, *1*(1), 150–166.

Atuduhor, R. R., Okpor, M. D., Yoro, R. E., Odiakaose, C. C., Emordi, F. U., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Ejeh, P. O., Abere, R. A., Ifioko, A. M., & Brizimor, S. E. (2024). StreamBoostE: A Hybrid Boosting-Collaborative Filter Scheme for Adaptive User-Item Recommender for Streaming Services. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *10*(2), 89–106. https://doi.org/10.22624/AIMS/V10N2P8

Bamashmos, S., Chilamkurti, N., & Shahraki, A. S. (2024). Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. *Sensors*, *24*(11). https://doi.org/10.3390/s24113575

Binitie, A. P., Akhator, D. N., & Chukwubueze, K. K. (2023). Design of a Resilient System against Shoulder Surfing Attack : Adaptable to USSD Channel. *Research Square*, 1–19. https://doi.org/10.21203/rs.3.rs-2793844/v1 License:

Binitie, A. P., & Babatunde, O. J. (2024). Evaluating the privacy issues, potential risks, and security measures associated with using social media platforms. *International Journal of African Research and Sustainability Studies*, *3*(2), 167–179.

Binitie, A. P., Odiakaose, C. C., Okpor, M. D., Ejeh, P. O., Eboka, A. O., Ojugo, A. A., Setiadi, D. R. I. M., Ako, R. E., Aghaunor, T. C., Geteloma, V. O., & Afotanwo, A. (2024). Stacked Learning Anomaly Detection Scheme with Data Augmentation for Spatiotemporal Traffic Flow. *Journal of Fuzzy Systems and Control*, *2*(3), 203–214. https://doi.org/10.59247/jfsc.v2i3.267

Binitie, A. P., Okofu, S. N., Okpor, M. D., Anazia, K. E., Ojugo, A. A., Egbokhare, F. A., Egwali, A., Ezzeh, P. O., Ako, R. E., Geteloma, V. O., Aghaunor, T. C., Ugbotu, E. V., & Onyemenem, S. I. (2025). MoBiSafe: an obfuscated single factor authentication mode to enhance secured USSD channel transaction in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *40*(1), 426. https://doi.org/10.11591/ijeecs.v40.i1.pp426-436

Bishop, M., Gates, C., Frincke, D., & Greitzer, F. L. (2009). AZALIA: An A to Z assessment of the likelihood of insider attack. *2009 IEEE Conference on Technologies for Homeland Security, HST 2009*, 385–392. https://doi.org/10.1109/THS.2009.5168063

Brizimor, S. E., Okpor, M. D., Yoro, R. E., Emordi, F. U., Ifioko, A. M., Odiakaose, C. C., Ojugo, A. A., Ejeh, P. O., Abere, R. A., Ako, R. E., & Geteloma, V. O. (2024). WiSeCart: Sensor-based Smart-Cart with Self-Payment Mode to Improve Shopping Experience and Inventory Management. *Social Informatics, Business, Politics, Law, Environmental Sciences and Technology Journal*, *10*(1), 53–74. https://doi.org/10.22624/aims/sij/v10n1p7

Cena, J. (2024). Multi-Factor Authentication Paradigms for Securing Industrial Internet of Multi-Factor Authentication Paradigms for Securing Industrial Internet of Things (IIoT) Assets. *Bulletin of Electrical Engineering and Informatics*, *21*(May), 23–46.

Deon, L., & Best, T. (2025). Zero Trust Security and Cloud Security : A Modern Approach to Cyberattack Prevention Date : February , 2025. *ResearchGate*, *1*(February). https://doi.org/10.13140/RG.2.2.24739.57126

Dwi, R. O. Z., & Asriningtias, Y. (2025). Real-Time Location Monitoring and Routine Reminders Based on Internet of Things Integrated with Mobile for Dementia Disorder. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *9*(1), 77–84. https://doi.org/10.29207/resti.v9i1.6105

Eboka, A. O., Aghware, F. O., Okpor, M. D., Odiakaose, C. C., Okpako, A. E., Ojugo, A. A., Ako, R. E., Binitie, A. P., Onyemenem, S. I., Ejeh, P. O., & Geteloma, V. O. (2025). Pilot study on deploying a wireless sensor-based virtual-key access and lock system for home and industrial frontiers. *International Journal of Informatics and Communication Technology*, *14*(1), 287–297. https://doi.org/10.11591/ijict.v14i1.pp287-297

Eboka, A. O., Odiakaose, C. C., Agboi, J., Okpor, M. D., Onoma, P. A., Aghaunor, T. C., Ojugo, A. A., Ugbotu, E. V., Max-Egba, A. T., Geteloma, V. O., Binitie, A. P., Onochie, C. C., & Ako, R. E. (2025). Resolving Data Imbalance Using a Bi-Directional Long-Short Term Memory for Enhanced Diabetes Mellitus Detection. *Journal of Future Artificial Intelligence and Technologies*, *2*(1), 95–109. https://doi.org/10.62411/faith.3048-3719-73

Ejeh, P. O., Nwankwo, O., Obaze, C. A., Linda, C., Onoma, P. A., Abere, R. A., & Aherobo, V. O. (2025). Data-Driven Framework for Strategic Knowledge Management to Enhance Organizational Learning : A Pilot Study. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *11*(4), 11–36. https://doi.org/10.22624/AIMS/BHI/V11N4P2

Ejeh, P. O., Okpor, M. D., Yoro, R. E., Ifioko, A. M., Onyemenem, S. I., Odiakaose, C. C., Ojugo, A. A., Ako, R. E., Emordi, F. U., & Geteloma, V. O. (2024). Counterfeit Drugs Detection in the Nigeria Pharma-Chain via Enhanced Blockchain-based Mobile Authentication Service. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *12*(2), 25–44. https://doi.org/10.22624/aims/maths/v12n2p3

Geteloma, V. O., Aghware, F. O., Adigwe, W., Odiakaose, C. C., Ashioba, N. C., Okpor, M. D., Ojugo, A. A., Ejeh, P. O., Ako, R. E., & Ojei, E. O. (2024a). AQuamoAS: unmasking a wireless sensor-based ensemble for air quality monitor and alert system. *Applied Engineering and Technology*, *3*(2), 70–85. https://doi.org/10.31763/aet.v3i2.1409

Geteloma, V. O., Aghware, F. O., Adigwe, W., Odiakaose, C. C., Ashioba, N. C., Okpor, M. D., Ojugo, A. A., Ejeh, P. O., Ako, R. E., & Ojei, E. O. (2024b). Enhanced data augmentation for predicting consumer churn rate with monetization and retention strategies: a pilot study. *Applied Engineering and Technology*, *3*(1), 35–51. https://doi.org/10.31763/aet.v3i1.1408

Geteloma, V. O., Okpor, M. D., Ugboh, E., Anazia, K. E., Odoh, A., Agboi, J., Abere, R. A., Aghaunor, T. C., Ugbotu, E. V., Odiakaose, C. C., & Ojugo, A. A. (2025). Investigating Risk Level in Maternal Mortality via a 3ConFA Feature Fused SMOTE-Tomek Balancing with Attention-Guided BiGRU Scheme : A Pilot Study. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *11*(3), 59–80. https://doi.org/10.22624/AIMS/BHI/V11N3P5x

Ifioko, A. M., Yoro, R. E., Okpor, M. D., Brizimor, S. E., Obasuyi, D. A., Emordi, F. U., Odiakaose, C. C., Ojugo, A. A., Atuduhor, R. R., Abere, R. A., Ejeh, P. O., Ako, R. E., & Geteloma, V. O. (2024). CoDuBoTeSS: A Pilot Study to Eradicate Counterfeit Drugs via a Blockchain Tracer Support System on the Nigerian Frontier. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *10*(2), 53–74. https://doi.org/10.22624/AIMS/BHI/V10N2P6

Jaber, A., & Fritsch, L. (2023). Towards AI-powered Cybersecurity Attack Modeling with Simulation Tools: Review of Attack Simulators. *Lecture Notes in Networks and Systems*, *571 LNNS*(October), 249–257. https://doi.org/10.1007/978-3-031-19945-5_25

Jose Diaz Rivera, J., Muhammad, A., & Song, W.-C. (2024). Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. *IEEE Open Journal of the Communications Society*, *5*, 2792–2814. https://doi.org/10.1109/OJCOMS.2024.3391728

Jose, J., Rivera, D., Akbar, W., Khan, T. A., & Muhammad, A. (2023). *Secure Enrollment Token Delivery Mechanism for Zero Trust Networks Using Secure enrollment token delivery mechanism for Zero Trust networks using blockchain ‡*. *July*. https://doi.org/10.1587/trans.E0.

Kaiser, A., Wageneder, E., & Kerschbaum, C. (2025). Advanced Spiritual Knowledge Management: Main Features of the Concept and Initial Ideas for Implementation in Schools and School Pastoral Care. *European Conference on Knowledge Management*, *26*(1), 499–506. https://doi.org/10.34190/eckm.26.1.3810

Krishna, V. V., Rupa, Y., Koushik, G., Varun, T., Kiranmayee, B. V., & Akhil, K. (2023). A Comparative Study on Authentication Vulnerabilities and Security Issues in Wearable Devices. *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023), Atlantis Highlights in Computer Sciences 18*, *18*(Icacecs), 106–116. https://doi.org/10.2991/978-94-6463-314-6_11

Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E., & Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). *NIPES - Journal of Science and Technology Research*, *6*(2), 293–311. https://doi.org/10.5281/zenodo.12617068

Malasowe, B. O., Akazue, M. I., Okpako, A. E., Aghware, F. O., Ojugo, A. A., & Ojie, D. V. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. *International Journal of Advanced Computer Science and Applications*, *14*(8), 135–142. https://doi.org/10.14569/IJACSA.2023.0140816

Malasowe, B. O., Edim, E. B., Adigwe, W., Okpor, M. D., Ako, R. E., Okpako, A. E., Ojugo, A. A., & Ojei, E. O. (2024). Quest for Empirical Solution to Runoff Prediction in Nigeria via Random Forest Ensemble: Pilot Study. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *10*(1), 73–90. https://doi.org/10.22624/aims/bhi/v10n1p8

Malasowe, B. O., Ojie, D. V., Ojugo, A. A., & Okpor, M. D. (2024). Co-Infection Prevalence of Covid-19 Underlying Tuberculosis Disease Using a Susceptible Infect Clustering Bayes Network. *Dutse Journal of Pure and Applied Sciences*, *10*(2), 80–94. https://doi.org/10.4314/dujopas.v10i2a.8

Malasowe, B. O., Okpako, A. E., Okpor, M. D., Ejeh, P. O., Ojugo, A. A., & Ako, R. E. (2024). FePARM: The Frequency-Patterned Associative Rule Mining Framework on Consumer Purchasing-Pattern for Online Shops. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *15*(2), 15–28. https://doi.org/10.22624/aims/cisdi/v15n2p2-1

Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial Intelligence (AI) and Internet of Medical Things (IoMT) Assisted Biomedical Systems for Intelligent Healthcare. *Biosensors*, *12*(8). https://doi.org/10.3390/bios12080562

Marasco, E., Albanese, M., Patibandla, V. V. R., Vurity, A., & Sriram, S. S. (2023). Biometric multi-factor authentication: On the usability of the FingerPIN scheme. *Security and Privacy*, *6*(1). https://doi.org/10.1002/spy2.261

Muhamada, K., Setiadi, D. R. I. M., Sudibyo, U., Widjajanto, B., & Ojugo, A. A. (2024). Exploring Machine Learning and Deep Learning Techniques for Occluded Face Recognition: A Comprehensive Survey and Comparative Analysis. *Journal of Future Artificial Intelligence and Technologies*, *1*(2), 160–173. https://doi.org/10.62411/faith.2024-30

Nur, M. J., Moses Setiadi, D. R. I., Ojugo, A. A., & Nguyen, M. T. (2025). Improving Customer Churn Prediction Using Domain-Driven Feature Engineering, Resampling, and CatBoost with Explainability Extensions. *2025 International Seminar on Application for Technology of Information and Communication (ISemantic)*, 493–499. https://doi.org/10.1109/ISemantic67418.2025.11291801

Obasuyi, D. A., Yoro, R. E., Okpor, M. D., Ifioko, A. M., Brizimor, S. E., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ako, R. E., Geteloma, V. O., Abere, R. A., Atuduhor, R. R., & Akiakeme, E. (2024). NiCuSBlockIoT: Sensor-based Cargo Assets Management and Traceability Blockchain Support for Nigerian Custom Services. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *15*(2), 45–64. https://doi.org/10.22624/aims/cisdi/v15n2p4

Odiakaose, C. C., Aghware, F. O., Okpor, M. D., Eboka, A. O., Binitie, A. P., Ojugo, A. A., Setiadi, D. R. I. M., Ibor, A. E., Ako, R. E., Geteloma, V. O., Ugbotu, E. V., & Aghaunor, T. C. (2024). Hypertension Detection via Tree-Based Stack Ensemble with SMOTE-Tomek Data Balance and XGBoost Meta-Learner. *Journal of Future Artificial Intelligence and Technologies*, *1*(3), 269–283. https://doi.org/10.62411/faith.3048-3719-43

Odiakaose, C. C., Omede, E. U., Anazia, K. E., Okpor, M. D., Ako, R. E., Aghaunor, T. C., Ugbotu, E. V., Ojugo, A. A., Moses Setiadi, D. R. I., Eboka, A. O., Max-Egba, A. T., Agboi, J., Onochie, C. C., & Onoma, P. A. (2025). Investigating Data Balancing Effects for Enhanced Behavioural Risk Detection in Cervical Cancer Using BiGRU: A Pilot Study. *NIPES - Journal of Science and Technology Research*, *7*(2), 319–329. https://doi.org/10.37933/nipes/7.2.2025.24

Odun-Ayo, I., Geteloma, V., Misra, S., Ahuja, R., & Damasevicius, R. (2020). *Systematic Mapping Study of Utility-Driven Platforms for Clouds* (pp. 762–774). https://doi.org/10.1007/978-3-030-30577-2_68

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Dependable Community-Cloud Framework for Smartphones. *American Journal of Networks and Communications*, *4*(4), 95. https://doi.org/10.11648/j.ajnc.20150404.13

Ojugo, A. A., & Eboka, A. O. (2018a). Assessing Users Satisfaction and Experience on Academic Websites: A Case of Selected Nigerian Universities Websites. *International Journal of Information Technology and Computer Science*, *10*(10), 53–61. https://doi.org/10.5815/ijitcs.2018.10.07

Ojugo, A. A., & Eboka, A. O. (2018b). Comparative Evaluation for High Intelligent Performance Adaptive Model for Spam Phishing Detection. *Digital Technologies*, *3*(1), 9–15. https://doi.org/10.12691/dt-3-1-2

Ojugo, A. A., & Eboka, A. O. (2018c). Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network. *Digital Technologies*, *3*(1), 1–8. https://doi.org/10.12691/dt-3-1-1

Ojugo, A. A., & Eboka, A. O. (2019a). Extending Campus Network Via Intranet and IP-Telephony For Better Performance and Service Delivery: Meeting Organizational Goals. *Journal of Applied Science, Engineering, Technology, and Education*, *1*(2), 94–104. https://doi.org/10.35877/454ri.asci12100

Ojugo, A. A., & Eboka, A. O. (2019b). Inventory prediction and management in Nigeria using market basket analysis associative rule mining: memetic algorithm based approach. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *8*(3), 128. https://doi.org/10.11591/ijict.v8i3.pp128-138

Ojugo, A. A., & Eboka, A. O. (2020a). An Empirical Evaluation On Comparative Machine Learning Techniques For Detection Of The Distributed Denial Of Service (DDoS) Attacks. *Journal of Applied Science, Engineering, Technology, and Education*, *2*(1), 18–27. https://doi.org/10.35877/454RI.asci2192

Ojugo, A. A., & Eboka, A. O. (2020b). Cluster prediction model for market basket analysis: quest for better alternatives to associative rule mining approach. *IAES International Journal of Artificial Intelligence*, *9*(3), 429–439. https://doi.org/10.11591/ijai.v9.i3.pp429-439

Ojugo, A. A., Ejeh, P. O., Akazue, M. I., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., Nwozor, B., & Emordi, F. U. (2023). CoSoGMIR: A Social Graph Contagion Diffusion Framework using the Movement-Interaction-Return Technique. *Journal of Computing Theories and Applications*, *1*(2), 163–173. https://doi.org/10.33633/jcta.v1i2.9355

Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Eboka, A. O., & Emordi, F. U. (2024). Predicting rainfall runoff in Southern Nigeria using a fused hybrid deep learning ensemble. *International Journal of Informatics and Communication Technology*, *13*(1), 108–115. https://doi.org/10.11591/ijict.v13i1.pp108-115

Ojugo, A. A., & Ekurume, E. (2021). Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2090–2102. https://doi.org/10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Nwankwo, O. (2021). Spectral-Cluster Solution For Credit-Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network. *JINAV: Journal of Information and Visualization*, *2*(1), 15–24. https://doi.org/10.35877/454ri.jinav274

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ako, R. E., Adigwe, W., Anazia, K. E., & Geteloma, V. O. (2023). Evidence of Students' Academic Performance at the Federal College of Education Asaba Nigeria: Mining Education Data. *Knowledge Engineering and Data Science*, *6*(2), 145. https://doi.org/10.17977/um018v6i22023p145-156

Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Ejeh, P. O., Adigwe, W., Anazia, K. E., & Nwozor, B. (2023). Forging a learner-centric blended-learning framework via an adaptive content-based architecture. *Science in Information Technology Letters*, *4*(1), 40–53. https://doi.org/10.31763/sitech.v4i1.1186

Ojugo, A. A., & Otakore, O. D. (2018). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. *Network and Communication Technologies*, *3*(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2020). Computational solution of networks versus cluster grouping for social network contact recommender system. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *9*(3), 185. https://doi.org/10.11591/ijict.v9i3.pp185-194

Ojugo, A. A., & Otakore, O. D. (2021). Forging An Optimized Bayesian Network Model With Selected Parameters For Detection of The Coronavirus In Delta State of Nigeria. *Journal of Applied Science, Engineering, Technology, and Education*, *3*(1), 37–45. https://doi.org/10.35877/454ri.asci2163

Ojugo, A. A., & Yoro, R. E. (2013). Computational Intelligence in Stochastic Solution for Toroidal N-Queen. *Progress in Intelligent Computing and Applications*, *1*(2), 46–56. https://doi.org/10.4156/pica.vol2.issue1.4

Ojugo, A. A., Yoro, R. E., Yerokun, M. O., & Iyawa, I. J. (2013). Implementation Issues of VoIP to Enhance Rural Telephony in Nigeria. *Journal of Emerging Trends in Computing and Information Sciences*, *4*(2), 172–179.

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence. *International Journal of Computer Applications*, *179*(39), 34–43. https://doi.org/10.5120/ijca2018916586

Okofu, S. N., Akazue, M. I., Oweimieotu, A. E., Ako, R. E., Ojugo, A. A., & Asuai, C. E. (2024). Improving Customer Trust through Fraud Prevention E-Commerce Model. *Journal of Computing, Science and Technoloogy*, *1*(1), 76–86.

Okofu, S. N., Anazia, K. E., Akazue, M. I., Okpor, M. D., Oweimieotu, A. E., Asuai, C. E., Nwokolo, G. A., Ojugo, A. A., & Ojei, E. O. (2024). Pilot Study on Consumer Preference, Intentions and Trust on Purchasing-Pattern for Online Virtual Shops. *International Journal of Advanced Computer Science and Applications*, *15*(7), 804–811. https://doi.org/10.14569/IJACSA.2024.0150780

Okonta, E. O., Ojugo, A. A., Wemembu, U. R., & Ajani, D. (2013). Embedding Quality Function Deployment In Software Development: A Novel Approach. *West African Journal of Industrial & Academic Research*, *6*(1), 50–64.

Okonta, E. O., Wemembu, U. R., Ojugo, A. A., & Ajani, D. (2014). Deploying Java Platform to Design A Framework of Protective Shield for Anti– Reversing Engineering. *West African Journal of Industrial & Academic Research*, *10*(1), 50–64.

Okpor, M. D., Aghware, F. O., Akazue, M. I., Eboka, A. O., Ako, R. E., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Geteloma, V. O., & Ejeh, P. O. (2024). Pilot Study on Enhanced Detection of Cues over Malicious Sites Using Data Balancing on the Random Forest Ensemble. *Journal of Future Artificial Intelligence and Technologies*, *1*(2), 109–123. https://doi.org/10.62411/faith.2024-14

Okpor, M. D., Aghware, F. O., Akazue, M. I., Ojugo, A. A., Emordi, F. U., Odiakaose, C. C., Ako, R. E., Geteloma, V. O., Binitie, A. P., & Ejeh, P. O. (2024). Comparative Data Resample to Predict Subscription Services Attrition Using Tree-based Ensembles. *Journal of Fuzzy Systems and Control*, *2*(2), 117–128. https://doi.org/10.59247/jfsc.v2i2.213

Okpor, M. D., Anazia, K. E., Adigwe, W., Okpako, A. E., Setiadi, D. R. I. M., Ojugo, A. A., Omoruwou, F., Ako, R. E., Geteloma, V. O., Ugbotu, E. V., Aghaunor, T. C., & Oweimieotu, A. E. (2025). Unmasking effects of feature selection and SMOTE-Tomek in tree-based random forest for scorch occurrence detection. *Bulletin of Electrical Engineering and Informatics*, *14*(3), 2393–2403. https://doi.org/10.11591/eei.v14i3.8901

Oladele, J. K., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Abere, R. A., Nwozor, B., Ejeh, P. O., & Geteloma, V. O. (2024). BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange. *Journal of Computing Theories and Applications*, *1*(3), 231–242. https://doi.org/10.62411/jcta.9509

Omede, E. U., Edje, A. E., Akazue, M. I., Utomwen, H., & Ojugo, A. A. (2024). IMANoBAS: An Improved Multi-Mode Alert Notification IoT-based Anti-Burglar Defense System. *Journal of Computing Theories and Applications*, *1*(3), 273–283. https://doi.org/10.62411/jcta.9541

Omoruwou, F., Ojugo, A. A., & Ilodigwe, S. E. (2024). Strategic Feature Selection for Enhanced Scorch Prediction in Flexible Polyurethane Form Manufacturing. *Journal of Computing Theories and Applications*, *1*(3), 346–357. https://doi.org/10.62411/jcta.9539

Omosor, J. C., Onoma, P. A., Ojugo, A. A., Ako, R. E., Geteloma, V. O., Akhutie-Anthony, P., & Okperigho, S. U. (2025). Security Enhancement using Multifactor Authentication Strategy for the Solenoid Door Access Control and Management: A Pilot Study. *FUPRE Journal of Scientific and Industrial Research*, *6*(3), 80–94.

Onoma, P. A., Agboi, J., Geteloma, V. O., Max-Egba, A. T., Eboka, A. O., Ojugo, A. A., Odiakaose, C. C., Ugbotu, E. V., Aghaunor, T. C., & Binitie, A. P. (2025). Investigating an Anomaly-based Intrusion Detection via Tree-based Adaptive Boosting Ensemble. *Journal of Fuzzy Systems and Control*, *3*(1), 90–97. https://doi.org/10.59247/jfsc.v3i1.279

Onoma, P. A., Agboi, J., Ugbotu, E. V., Aghaunor, T. C., Odiakaose, C. C., Ojugo, A. A., Eboka, A. O., Binitie, A. P., Ezzeh, P. O., Ejeh, P. O., Onochie, C. C., Geteloma, V. O., Emordi, F. U., Orobor, A. I., & Obruche. (2025). Attrition Rate Prediction using a Frequency-Recency- Monetization-based SMOTEEN-Boosted Approach. *MSIS - International Journal of Advanced Computing and Intelligent System*, *3*(1), 1–11.

Onoma, P. A., Ako, R. E., Anazia, K. E., Oghorodi, D., Okpako, A. E., Onochie, C. C., Geteloma, V. O., Ezzeh, P. O., Ugboh, E., Ojugo, A. A., Eboka, A. O., & Idama, R. O. (2025). Quest for Ground-Truth or Stochastic Myth by Leveraging the AI-Powered Wearable Device for Dementia Disease Detection: A Pilot Study. *FUPRE Journal of Scientific and Industrial Research*, *9*(3), 343–358.

Onoma, P. A., Ako, R. E., Ojugo, A. A., Geteloma, V. O., Akhutie-Anthony, P., & Okperigho, S. U. (2025). Dementia Detection and Management using Wearable Device fused Deep Learning Scheme. *FUPRE Journal of Scientific and Industrial Research*, *6*(3), 80–94.

Onoma, P. A., Ugbotu, E. V., Aghaunor, T. C., Agboi, J., Ojugo, A. A., Odiakaose, C. C., Max-Egba, A. T., Niemogha, S. U., Binitie, A. P., & Abdullahi, M. B. (2025). Voice-based Dynamic Time Warping Recognition Scheme for Enhanced Database Access Security. *Journal of Fuzzy Systems and Control*, *3*(1), 81–89. https://doi.org/10.59247/jfsc.v3i1.293

Otorokpo, E. A., Okpor, M. D., Yoro, R. E., Brizimor, S. E., Ifioko, A. M., Obasuyi, D. A., Odiakaose, C. C., Ojugo, A. A., Atuduhor, R. R., Akiakeme, E., Ako, R. E., & Geteloma, V. O. (2024). DaBO-BoostE: Enhanced Data Balancing via Oversampling Technique for a Boosting Ensemble in Card-Fraud Detection. *Advances in Multidisciplinary & Scientific Research Journal Publications*, *12*(2), 45–66. https://doi.org/10.22624/aims/maths/v12n2p4

Oyemade, D. A., Akpojaro, J., Ojugo, A. A., Ureigho, R. J., Imouokhome, F. A.-A., & Omoregbee, E. U. (2016). A Three Tier Learning Model for Universities in Nigeria. *Journal of Technologies in Society*, *12*(2), 9–20. https://doi.org/10.18848/2381-9251/cgp/v12i02/9-20

Oyemade, D. A., & Ojugo, A. A. (2020). A Property Oriented Pandemic Surviving Trading Model. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(5), 7397–7404. https://doi.org/10.30534/ijatcse/2020/71952020

Oyemade, D. A., & Ojugo, A. A. (2021). An Optimized Input Genetic Algorithm Model for the Financial Market. *International Journal of Innovative Science, Engineering and Technology, 8*(2), 408–419. https://ijiset.com/vol8/v8s2/IJISET_V8_I02_41.pdf

Pratama, N. R., Setiadi, D. R. I. M., Harkespan, I., & Ojugo, A. A. (2025). Feature Fusion with Albumentation for Enhancing Monkeypox Detection Using Deep Learning Models. *Journal of Computing Theories and Applications*, *2*(3), 427–440. https://doi.org/10.62411/jcta.12255

Quamara, S., & Singh, A. K. (2023). An In-depth Security and Performance Investigation in Hyperledger Fabric-configured Distributed Computing Systems. *Blockchain Models*, *1*(1), 12–24.

Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2). *Health and Technology*, *12*(5), 923–929. https://doi.org/10.1007/s12553-022-00691-6

Rehman, N. (2024). *Strengthening Financial Institutions ' Data Security with Blockchain Technology and Zero Trust Security : A Comprehensive Cyber Defense Strategy Date : November , 2024*. *November*. https://doi.org/10.13140/RG.2.2.21956.85127

Salam, A., Abrar, M., Amin, F., Ullah, F., Khan, I. A., Alkhamees, B. F., & Alsalman, H. (2024). Securing Smart Manufacturing by Integrating Anomaly Detection with Zero-Knowledge Proofs. *IEEE Access*, *12*, 36346–36360. https://doi.org/10.1109/ACCESS.2024.3373697

Samuel Onimisi Dawodu, Adedolapo Omotosho, Odunayo Josephine Akindote, Abimbola Oluwatoyin Adegbite, & Sarah Kuzankah Ewuga. (2023). Cybersecurity Risk Assessment in Banking: Methodologies and Best Practices. *Computer Science & IT Research Journal*, *4*(3), 220–243. https://doi.org/10.51594/csitrj.v4i3.659

Setiadi, D. R. I. M., Muslikh, A. R., Irianandа, S. W., Warto, W., Gondohanindijo, J., & Ojugo, A. A. (2024). Outlier Detection Using Gaussian Mixture Model Clustering to Optimize XGBoost for Credit Approval Prediction. *Journal of Computing Theories and Applications*, *2*(2), 244–255. https://doi.org/10.62411/jcta.11638

Setiadi, D. R. I. M., Ojugo, A. A., Pribadi, O., Kartikadarma, E., Setyoko, B. H., Widiono, S., Robet, R., Aghaunor, T. C., & Ugbotu, E. V. (2025). Integrating Hybrid Statistical and Unsupervised LSTM-Guided Feature Extraction for Breast Cancer Detection. *Journal of Computing Theories and Applications*, *2*(4), 536–552. https://doi.org/10.62411/jcta.12698

Setiadi, D. R. I. M., Rustad, S., Sutojo, T., Akrom, M., Nguyen, M. T., Afendee, M., Sambas, A., & Ojugo, A. A. (2026). Hyperchaotic cross-coupled quantum 2D maps with interdependent rotational asymmetry for secure image encryption. *Optics Communications*, *600*(November 2025), 1–17. https://doi.org/10.1016/j.optcom.2025.132699

Setiadi, D. R. I. M., Susanto, A., Nugroho, K., Muslikh, A. R., Ojugo, A. A., & Gan, H. S. (2024). Rice Yield Forecasting Using Hybrid Quantum Deep Learning Model. *Computers*, *13*(8). https://doi.org/10.3390/computers13080191

Setiadi, D. R. I. M., Sutojo, T., Rustad, S., Akrom, M., Ghosal, S. K., Nguyen, M. T., & Ojugo, A. A. (2025). Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps: An Ultra-Wide Range Dynamics for Image Encryption. *Computers, Materials and Continua*, *83*(2), 2161–2188. https://doi.org/10.32604/cmc.2025.063729

Sinha, S. (2024). Blockchain for Enhancing IoT Privacy and Security. *International Journal of Innovative Research in Computer Science and Technology*, *12*(2), 106–110. https://doi.org/10.55524/ijircst.2024.12.2.18

Ugbotu, E. V., Aghaunor, T. C., Agboi, J., Max-Egba, A. T., Onoma, P. A., Geteloma, V. O., Eboka, A. O., Binitie, A. P., Ako, R. E., Nwozor, B., Onochie, C. C., Ojugo, A. A., Jumbo, E. F., Oweimieotu, A. E., & Odiakaose, C. C. (2025). Transfer Learning Using a CNN Fused Random Forest for SMS Spam Detection with Semantic Normalization of Text Corpus. *NIPES - Journal of Science and Technology Research*, *7*(2), 371–382. https://doi.org/10.37933/nipes/7.2.2025.29

Ugbotu, E. V., Emordi, F. U., Ugboh, E., Anazia, K. E., Odiakaose, C. C., Onoma, P. A., Idama, R. O., Ojugo, A. A., Geteloma, V. O., Oweimieotu, A. E., Aghaunor, T. C., Binitie, A. P., Odoh, A., Onochie, C. C., Ezzeh, P. O., Eboka, A. O., Agboi, J., & Ejeh, P. O. (2025). Investigating a SMOTE-Tomek Boosted Stacked Learning Scheme for Phishing Website Detection: A Pilot Study. *Journal of Computing Theories and Applications*, *3*(2), 145–159. https://doi.org/10.62411/jcta.14472

Wemembu, U. R., Okonta, E. O., Ojugo, A. A., & Okonta, I. L. (2014). A Framework for Effective Software Monitoring in Project Management. *West African Journal of Industrial and Academic Research*, *10*(1), 102–115.

Wu, J., Xue, N., Li, Z., Hong, X., Zhao, Y., Huang, X., & Zhang, J. (2024). SPCL: A Smart Access Control System That Supports Blockchain. *Applied Sciences*, *14*(7), 2978. https://doi.org/10.3390/app14072978

Yadalam, P. K., Shenoy, S. B., Anegundi, R. V., Mosaddad, S. A., & Heboyan, A. (2024). Advanced machine learning for estimating vascular occlusion percentage in patients with ischemic heart disease and periodontitis. *International Journal of Cardiology: Cardiovascular Risk and Prevention*, *21*(May), 0–3. https://doi.org/10.1016/j.ijcrp.2024.200291

Yoro, R. E., & Ojugo, A. A. (2019a). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. *American Journal of Modeling and Optimization*, *7*(2), 35–41. https://doi.org/10.12691/ajmo-7-2-1

Yoro, R. E., & Ojugo, A. A. (2019b). Quest for Prevalence Rate of Hepatitis-B Virus Infection in the Nigeria: Comparative Study of Supervised Versus Unsupervised Models. *American Journal of Modeling and Optimization*, *7*(2), 42–48. https://doi.org/10.12691/ajmo-7-2-2

Yoro, R. E., Okpor, M. D., Akazue, M. I., Okpako, A. E., Eboka, A. O., Ejeh, P. O., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Ako, R. E., Geteloma, V. O., Onoma, P. A., Max-Egba, A. T., Ibor, A. E., Onyemenem, S. I., & Ukwandu, E. (2025). Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner. *Plos One*, *20*(6 June), 1–20. https://doi.org/10.1371/journal.pone.0326571

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

Zhang, Z., Zhu, Z., Wang, X., Liu, D., Liu, X., Mi, Z., Tao, H., & Fan, H. (2023). Comprehensive landscape of immune-based classifier related to early diagnosis and macrophage M1 in spinal cord injury. *Aging*, *15*(4), 1–19. https://doi.org/10.18632/aging.204548

Zuama, L. R., Setiadi, D. R. I. M., Susanto, A., Santosa, S., Gan, H. S., & Ojugo, A. A. (2025). High-Performance Face Spoofing Detection using Feature Fusion of FaceNet and Tuned DenseNet201. *Journal of Future Artificial Intelligence and Technologies*, *1*(4), 385–400. https://doi.org/10.62411/faith.3048-3719-62