Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 17 No. 1, March 2026 - www.cisdijournal.net

Trust-constrained Intelligence for Realtime Clinical Reasoning in Centralized Healthcare Information Systems: A Pilot Study

[1]Ejeh, Patrick Ogholuwarami, [2]Onyekweli Osilonya Vincent & [3]Isizoh Anthony
[1]Faculty of Computing, Dennis Osadebay University Asaba, Nigeria
[2]Faculty of Computing, Novena University Ogume, Nigeria
[3]Faculty of Computing, Nnamdi Azikiwe University Awka, Nigeria
E-mails: patrick.ejeh@dou.edu.ng, osilanyavincent@gmail.com, anthonyisizoh@yahoo.com

ABSTRACT

We advance a trust-governed clinical decision support architecture designed for centralized healthcare information environments. Existing centralized systems such as Clinical Patient Information Systems (CPIS) offer rich data integration but often lack safeguards that ensure automated intelligence is deployed responsibly. To address this gap, the study proposes a layered framework that treats inference as a supervised institutional function rather than a detached algorithmic computation. The model combines tightly regulated clinical data ingestion, parallel ensemble-based predictive reasoning, latency-aware aggregation, and a trust enforcement layer that verifies user legitimacy, clinical context, and institutional policy alignment prior to alert delivery. Unlike conventional CDSS implementations that emphasize accuracy metrics in isolation, the presented approach frames decision support as a time-bound and policy-constrained workflow. The reasoning engine employs tree-based and probabilistic models to capture heterogeneous patterns in structured patient data, while the trust layer controls intelligence emission through real-time validation and audit metadata generation. Empirical motivation and literature support illustrate that such integration enhances interpretability, strengthens clinician confidence, and mitigates misuse or automation bias. The architecture aligns computational deliverables with governance requirements, demonstrating that safety and reliability emerge from system design choices rather than post-hoc oversight alone. By embedding measurement instrumentation for latency and access provenance, the system enables transparent evaluation and future extensibility. Overall, the study contributes a replicable path toward accountable, auditable, and operationally viable CDSS deployment within centralized institutional infrastructures.

Keywords: Clinical Decision Support Systems, Trust Governance, Electronic Health Record, Safety Latency-Constrained, Ensemble Inference, Clinical Data Security

CISDI Journal Reference Format
Ejeh, P.O., Onyekweli, O.V. & Isizoh, A. (2026): Trust-constrained Intelligence for Realtime Clinical Reasoning in Centralized Healthcare Information Systems: A Pilot Study. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 17 No 1, Pp 1-24. Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V17N1P1x

1. BACKGROUND TO THE STUDY

Contemporary healthcare delivery is increasingly mediated by systems that transform raw clinical data into actionable knowledge at the point of care (Abdulmalik & Yassin, 2023; Ejeh et al., 2025). The widespread use of centralized electronic health records has enabled unprecedented levels of data aggregation, longitudinal patient tracking, and institutional-scale analytics (Sheng et al., 2023).

It reshapes operationalized clinical decisions as used in hospitals and large health networks (Aghware, Okpor, et al., 2024; Olaniyi et al., 2023). And promises an improved diagnostic accuracy, standardized care delivery, and enhanced patient safety through timely access to comprehensive clinical records. The availability of structured EHR has also accelerated the integration of machine learning decision support that augments clinician judgment with predictions (Onoma, Ako, Anazia, Oghorodi, et al., 2025; Onoma, Ako, Ojugo, Geteloma, et al., 2025). Despite these advances, a growing body of evidence suggests that clinical value of intelligent decision support is not determined by predictive accuracy alone. Studies consistently report that delayed alerts, opaque behavior, and weak governance schemes can undermine clinician trust and, in some cases, advance new safety risks (Binitie et al., 2024, 2025, 2026). Timeliness and accountability emerge as determinants of clinical effectiveness rather than just a concern. In healthcare where decisions are time-critical, delays in alert generation can render predictions clinically irrelevant, especially in scenarios like abnormal detection, safety monitor, and early warnings (Finlow-bates, 2020; Ojugo et al., 2024). Thus, latency transforms from a technical metric into a clinical risk factor that impacts patient outcome and workflow efficiency (Binitie et al., 2026).

The governance of access and decision has become increasingly salient also – for de-escalating security and privacy threats. Medical data repositories are high-value targets (Li et al., 2025), and breaches of unauthorized access, privilege escalation, or misuse of legitimate credentials are widely documented across healthcare settings (Aghware, Ojugo, et al., 2024; Omede et al., 2024). Security models leverage continuous verification and strict access control to dissuade access to health information (Setiadi, Muslikh, et al., 2024; Setiadi, Rustad, et al., 2025). These approaches emphasize role-based access, multifactor authentication (MFA), and enforcement to ensure that every interaction with clinical data is authenticated, authorized, and auditable (Agrafiotis et al., 2015; Ibrahim & Ali, 2023). Such mechanisms are essential for regulatory compliance and institutional accountability. However, existing implementations focus narrowly on data access rather than on the legitimacy and traceability of automated clinical decisions themselves. In addition, methodological limitations persist, and studies show that predictive models evaluated under offline conditions (Akazue et al., 2023, 2024; San et al., 2025) yields strong performance as they exhibit brittleness with the heterogeneity, noise, and missingness that characterize realtime EHR (Aghaunor et al., 2026; Sun & Gu, 2021; Ugbotu, Aghaunor, et al., 2025; Ugbotu, Ako, et al., 2025). Also, single model are vulnerable to overfitting and instability, especially when deployed across evolving patient populations and changing clinical practices. As such, reliance on a single learner may inadvertently amplify diagnostic uncertainty rather than mitigate it (Okeke & Omojola, 2025).

Ensemble learning has emerged as a strategy for stabilizing predictions and improving robustness in complex clinical domains. Prior studies demonstrate that combining multiple models can reduce variance, capture complementary data patterns, and yield more reliable probability estimates (Onoma, Agboi, Ugbotu, et al., 2025; Onoma, Ako, Anazia, Oghorodi, et al., 2025). Ensembles have been known to outperform standalone models across a range of tasks including disease classification (Aghaunor, Agboi, et al., 2025; Aghaunor, Omede, et al., 2025; Nur et al., 2025). Existing ensemble prioritize predictive gains not accounting for inference latency or governance constraints imposed by the infrastructure. Thus, machine learning have outpaced the progress in integration and operational validation with current research targeted at a fragmentation between three critical dimensions (Oyemade et al., 2016; Oyemade & Ojugo, 2021) as thus: (a) first, predictive intelligence from temporal constraints define clinical relevance (Onoma, Ako, Ojugo, Geteloma, et al., 2025), (b) next, security and access control mechanisms become protective wrappers around repositories of decision support (Ojugo & Eboka, 2019), and (c) lastly – ensemble reasoning is largely framed as a performance optimization for managing epistemic risk and uncertainty in safe-critical environs (Tahir et al., 2025). Without a unifying framework, these remain loosely coupled, limiting the translational impact. Motivated by these, our study addresses gap in the deployment of clinical decision support systems with centralized health data (Agboi, Emordi, et al., 2025; Agboi, Onoma, et al., 2025). Lack in handling integrated scheme for temporal responsiveness, trust enforcement, and collective model reasoning as coequal constraint in a system has continued to hamper and degrade system performance as demonstrated in centralized architectures for achieving low latency and high availability in healthcare settings (Aghware et al., 2023, 2025). While, studies note the benefits of continuous verification and formalized access control – others, examine how decision support is realized under simultaneous constraints of timeliness, accountability, and predictive reliability.

We advance clinical intelligence, conceptualized as governed, time-bounded reasoning process within the centralized healthcare infrastructures. We rationalize access control, latency management, and ensemble inference as peripheral implementation; And also position them as first class design principles that jointly determine clinical utility. Thus, our study addresses: (a) how to improve prediction accuracy, (b) deliver timely clinical decisions, and (c) provide an EHR that is traceable, auditable, and trustworthy in realtime operational constraints. The study contributes thus – (a) articulates a system level formulation of trust constrained clinical reasoning that explicitly integrates access governance and temporal requirements into the decision process (Allenotor et al., 2015; Allenotor & Ojugo, 2017), (b) advance a multi inference framework that leverages collective reasoning to stabilize predictions with end-to-end latency constraints inherent in centralized clinical data systems (Ako et al., 2024, 2025), and (c) demonstrate that governed intelligence is achieved without compromising real time responsiveness or compliance requirements (Atuduhor et al., 2024; Brizimor et al., 2024; Obasuyi et al., 2024). The study bridges real-time machine learning with architectural and security considerations that are often treated separately by previous studies. The remainder of the paper is organized as follows. The next section presents a critical synthesis of related work in intelligent clinical decision support, centralized healthcare systems, and security governance. Section three formalizes system model and problem definition underlying trust-constrained clinical reasoning. Section four details the proposed method and implementation framework. Section five reports experimental results and performance analysis. Section six discusses the implications of the findings in relation to existing approaches. Finally, Section seven concludes the paper and outlines directions for future research.

2. REVIEW OF RELATED WORKS

The evolution of intelligent clinical decision support systems (CDSS) is closely tied to data availability, computational capacity, and machine learning methodologies (Odiakaose et al., 2024, 2025). Early CDSS were largely rule-based, relying on manually encoded expert knowledge/guidelines to trigger recommendations (Li et al., 2024; Lötsch et al., 2022). While these systems offered transparency and interpretability, they struggled to scale across complex clinical scenarios and heterogeneous patient populations. The subsequent integration of data-driven learning models marked a significant paradigm shift, enabling predictive analytics derived from EHR data (Ibor et al., 2023; Oladele et al., 2024). Thus, intelligence from CDSS moved from static knowledge representation to adaptive inference grounded in empirical clinical data. Recent studies now explore a wide range of learning schemes for clinical prediction (Muhamada et al., 2024; Pratama et al., 2025; Zuama et al., 2025).

These have demonstrated great success in disease risk stratification, patient outcome, and early warning systems (Ojugo et al., 2024; Ojugo, Akazue, Ejeh, Ashioba, Odiakaose, et al., 2023; Ojugo, Allenotor, et al., 2015; Ojugo, Odiakaose, Emordi, Ejeh, et al., 2023). Many of these focus primarily on accuracy. As such, system level constraints related to real time inference, integration overhead, and deployment latency are often under examined. Without a doubt, this methodological emphasis limits the translational relevance of many proposed solutions. A particularly persistent limitation in CDSS is its reliance on single model inference (Ojugo & Eboka, 2018c, 2018b, 2018a). Although single learners offer simplicity and ease interpretation – they are often susceptible to noise, distributional shifts, imbalance in dataset, and feature instability; all of which are common in real-world clinical environments (Ojugo & Nwankwo, 2021a, 2021b, 2021c). These have also been found to degrade generalization significantly across patient dataset that differ from the training population, raising concerns about reliability and generalizability. These findings have motivated growing interest in ensemble learning as a mechanism for mitigating uncertainty and improving robustness (Setiadi, Muslikh, et al., 2024; Setiadi, Ojugo, et al., 2025).

Ensemble-based CDSS fuses predictions from multi-model to reduce variance and capture decision patterns (Onoma, Ako, Anazia, Oghorodi, et al., 2025; Onoma, Ako, Ojugo, Geteloma, et al., 2025). Ensembles often outperforms individual classifiers in terms of stability and predictive consistency, particularly when dealing with high dimensional EHR features (Palanisamy & Thirunavukarasu, 2019). Most ensemble emphasize predictive gains that treat inference latency as a secondary concern. Others quantify end-to-end decision delay introduced by multi-model execution, aggregation, and post processing as clinically impactful in time-sensitive scenarios (Onoma, Agboi, Geteloma, et al., 2025; Onoma, Agboi, Ugbotu, et al., 2025). Beyond the intelligence in ensembles, the architecture of EHRs plays an insightful role in shaping CDSS performance and adoption. Health information infrastructures and widely-used EHRs are due to their ability to provide unified access, consistent policy enforcement, and centralized auditing (Geteloma et al., 2024a, 2024b, 2025).

While, previous studies yield simplified interoperability, reduce data duplication, and enable organization-wide analytics that are difficult in fragmented systems – such centralized infrastructures are the dominant substrate for intelligent CDSS as deployed today. However, centralization also introduces performance and governance challenges. High volumes of concurrent access, complex role hierarchies, and heterogeneous clinical workflows can strain system responsiveness, particularly when advanced analytics are integrated into the data access pipeline (Atuduhor et al., 2024). Studies have reported poorly optimized centralized systems birth alert delays that disrupt clinician workflows, and reduce trust recommendations (Yoro et al., 2025; Yoro & Ojugo, 2019a, 2019b). This also, amplifies the importance of latency management and efficient decision pipelines, yet these aspects are rarely examined in conjunction with machine learning model design.

Security and governance mechanisms represent a third critical domain shaping the effectiveness of intelligent clinical systems. Healthcare IT environments are subject to stringent regulatory requirements and face persistent threats ranging from insider misuse to external cyber-attacks (Folorunso, 2024; Bala et al., 2024). To address these risks, access control frameworks based on role based access control, multifactor authentication, and encryption have become standard components of modern EHRs (Zhang et al., 2022; Zuama et al., 2025). More recently, Zero Trust inspired models have been proposed to enforce continuous verification and minimize implicit trust within healthcare networks (Setiadi, Susanto, et al., 2024; Setiadi, Sutojo, et al., 2025).

While these strengthens data protection, they are limited in scope to control who can access data, and how automated decisions are generated, validated, and acted upon. Existing models rarely address decision provenance, model accountability, or model recommendations traceability in the CDSS (Ojugo, Akazue, Ejeh, Ashioba, Odiakaose, et al., 2023; Ojugo, Odiakaose, Emordi, Ejeh, et al., 2023). Thus, a clinician may receive a technically, authorized automated alert that lacks transparent linkage to verified context, timing constraints, or model agreement. This gap is problematic as recommendations increasingly influence all clinical judgments. CDSS research prioritizes predictive performance, centralized system studies emphasize data management and interoperability, and security research focuses on access enforcement and compliance. Without a doubt, each strand contributes valuable insights, yet their separation obscures critical interactions that determine real world clinical effectiveness (Malasowe, Aghware, et al., 2024; Malasowe, Edim, et al., 2024). Alert latency, clinician trust, and decision accountability emerge at the intersection of these domains, but remain insufficiently addressed by existing approaches.

System Model

With our objective to define how intelligent clinical inference operates when subject to explicit governance and temporal requirements, we thus establish the rigorous foundation that defines our CDSS as a tuple in Equation 1 – where D is a set of clinical records attributes and derived clinical features, U is all users interacting with the system, R are roles defined for all assigned to users, P are all access and decision policies that govern permissible actions under specific contextual conditions, and A is the set of authorized actions, including data access, model invocation, and clinical alert dissemination (Polge et al., 2021; Sheikhtaheri & Sabermahani, 2022).

$$H = (D, U, R, P, A) \quad Equation\ 1$$

Centralized healthcare infrastructures rely on this formal separation between users, roles, and policies to enforce accountability and regulatory compliance, as widely documented in prior healthcare IT studies (Janett and Yeracaris, 2020; Omotayo et al., 2021; Rahman and Jim, 2024). In essence, the tuple formulation allows system behavior to be reasoned about formally, which is critical for clinical environments as in Equation 2. Clinical inference within this system is modeled as a probabilistic function where a patient feature vector in a d dimensional space is mapped to a continuous risk score representing the likelihood of a clinical condition or adverse outcome.

$$f: \mathbb{R}^d \to [0,1] \quad Equation\ 2$$

This formulation aligns with prior machine learning based CDSS models that frame clinical prediction as a risk estimation task rather than a deterministic classification problem (Okofu, Akazue, et al., 2024; Okofu, Anazia, et al., 2024). However, unlike conventional formulations, inference in this work is not unconstrained. Two classes of constraints govern the validity of any inferred decision. The first are trust constraints, which require that the requesting user is authenticated, holds a valid role assignment, and satisfies all relevant access policies at the time of inference (Ojugo & Yoro, 2013, 2020). These constraints are informed by role-based access control as well as the continuous verification. An inference result that violates any trust condition is considered invalid regardless of its predictive confidence.

The second class are temporal constraints. Let T_f denote the end-to-end time required to execute data retrieval, model inference, aggregation, and alert generation as in Equation 3 where τ represents the clinically acceptable response time defined by workflow requirements and domain-specific urgency.

$$T_f \leq \tau \qquad Equation\ 3$$

Prior studies emphasize that alerts delivered outside clinically meaningful time windows erode clinician trust and reduce adoption of CDSS tools (Hydari et al., 2019; Johnson et al., 2021; Schaut et al., 2022). Thus, latency is treated as a hard constraint rather than an optimization objective. The problem addressed in this study can therefore be stated as follows. Given a centralized health information system H and a stream of patient feature vectors, design a decision support mechanism that maximizes predictive reliability while satisfying all trust and temporal constraints. Predictive reliability is understood as the stability and consistency of inferred risk scores across heterogeneous data conditions, rather than peak accuracy alone, consistent with findings from ensemble learning research in healthcare (Malasowe et al., 2023; Malasowe, Okpako, et al., 2024). To operationalize this formulation, we introduce algorithms 1 that governs trust validated inference execution, and also algorithm 2 that performs constrained ensemble aggregation under latency bounds.

Algorithm 1: Trust Validated Clinical Inference

```
Input: User u, patient features x, system tuple H
Output: Validated risk score or null
Verify authentication state of u
Retrieve role r assigned to u
Evaluate policy set P for action request
If any trust check fails then return null
Retrieve clinical data D relevant to x
Invoke inference pipeline with x
Return provisional inference result
```

Algorithm 2: Time Bounded Ensemble Risk Estimation

```
Input: Feature vector x, model set M, time bound τ
Output: Aggregated risk score f(x)
Start system timer
For each model m in M do
    Compute risk score rm(x)
    If elapsed time exceeds τ then break
Aggregate available risk scores
Normalize aggregated output
If total time ≤ τ then return f(x)
Else return null
```

3. METHODOLOGY

Aligned computational intelligence with centralized system governance as in Figure 1 – it consists of 4-stages namely: (a) centralized data ingestion, (b) parallel model-based reasoning, (c) trust and policy enforcement, and (d) decision emission. Each stage explicitly supports traceability, latency measurement, and access audit that ensures both clinical relevance and regulatory compliance (Okonta et al., 2013, 2014; Wemembu et al., 2014).

1. Centralized data ingestion is the entry point for inference requests, retrieving structured patient records and derived features from the EHR repository. This leverages the consistency and integrity of the CDSS as shown to support reliable analytics and institutional oversight. Data access is constrained via its unified interface so that the framework can avoid fragmentation and uncontrolled model invocation that degrades accountability in distributed deployments.
2. The inference (reasoning engine) operates as a governed service rather than a freely callable function. Requests are accepted only after preliminary validation of user identity and role context, after which feature vectors are dispatched to the clinical reasoning engine. Inference becomes a policy-aware task that aligns decision support with organizational authority structures. The clinical reasoning engine implements collective inference via parallel execution of multiple predictive models (Anthony-Akhutie et al., 2025). Unlike single learner CDSS designs, this engine is constructed to manage uncertainty and variability inherent in EHRs data. Each model operates on the same patient feature vector, to yield a probabilistic risk estimate that reflects the learned clinical patterns as in Figure 2. Our choice of tree-based classifiers is demonstrated in its effectiveness to handle all structured healthcare datasets and their relatively inference latency profiles (Aleisa et al., 2025). Also, they capture nonlinear feature interactions, yield robustness, and calibrate risk estimates that support downstream aggregation. These inductive biases, helps to reduce its reliance assumption on a single model, while aggregation computed via composite risk score for improved robustness is not achieved at the expense of clinical timeliness. Its ensemble reasoning is reframed from a performance optimization mode into a form of epistemic risk management, consistent with findings that collective inference improves stability under heterogeneous data conditions (Ojugo & Eboka, 2020a, 2020b). Importantly, the reasoning engine is stateless with respect to user identity and access control. This separation of concerns allows model behavior to remain consistent and testable, while governance decisions are enforced externally. Such modularity improves reproducibility and simplifies validation, addressing concerns raised in prior CDSS studies regarding opaque and tightly coupled implementations (Quamara & Singh, 2023; Salam et al., 2024; San et al., 2025).

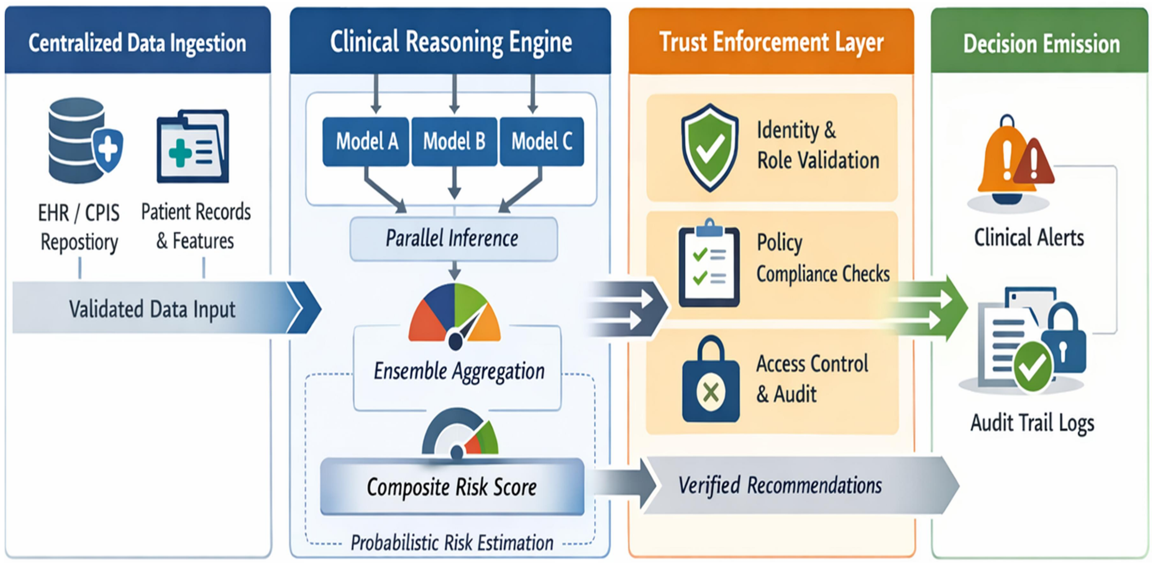

Figure 1: High-Level Overview of the Trust-Constrained Clinical Decision Support Framework

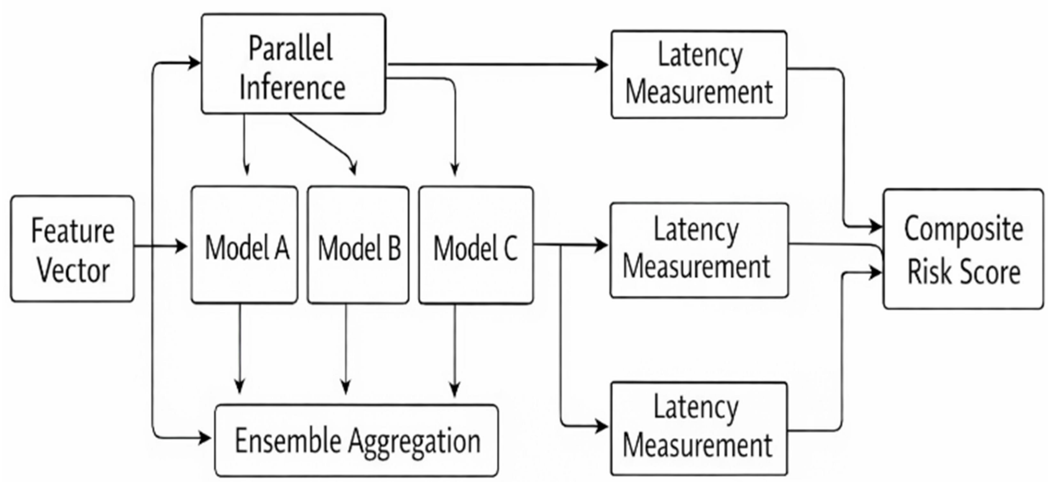

Figure 2: Parallel Ensemble Inference And Aggregation Process Under Latency Constraints

3. The trust enforcement layer acts as a decision gate that mediates between raw inference outputs and actionable clinical alerts. This layer continually verifies authentication state, role validity, and contextual authorization of the requesting user at the time of decision release – and governs the emission of intelligence. Continuous verification is essential in centralized healthcare environments where user context may change dynamically due to shifts, emergency overrides, or role escalation (Jabbar et al., 2021; Jose et al., 2023). Re-evaluating trust states prior to alert delivery ensures system ensures recommendations are accurate, legitimate and auditable. An inference result that fails trust validation is suppressed, regardless of its predictive confidence, thereby prioritizing governance over opportunistic intelligence.

Decision provenance metadata, including model identifiers, aggregation timestamps, and access context, is attached to every released alert. This design supports post hoc auditing and aligns with calls in the healthcare security literature for greater accountability in automated decision making systems (Hakonen, 2022; Ifioko et al., 2024). In essence, trust enforcement transforms CDSS outputs from opaque suggestions into traceable institutional actions (Habib et al., 2022).

Architecture and Deployment Design

While this architecture reflects the integration of intelligence, infrastructure, and governance unified – it is logically centralized, and serves as EHR platform data source and access control anchor. The clinical reasoning engine and trust enforcement services are modularly deployed in the same controlled environment, minimizing network induced latency and simplifying policy enforcement. This choice is consistent with prior evidence that centralized deployments simplify interoperability and auditing; whilst supporting low latency analytics if properly optimized (Okpor et al., 2024, 2025). It reduces surface attacks via unnecessary distribution of inference services, which is crucial in clinical workflows. All components are containerized and executed within a controlled runtime environment aligned with the centralized healthcare infrastructure. Latency tracing is embedded at each stage of the decision pipeline, capturing data retrieval time, per model inference duration, aggregation overhead, and trust enforcement delay (Ojugo & Otakore, 2018, 2021).

Access logs, authentication, policy evaluations, and alert delivery enables fine-grained analysis of both performance and governance. Thus, model addresses directly the gaps in previous works with alert delays and trust erosion (Omoruwou et al., 2024; Omosor et al., 2025; Otorokpo et al., 2024).

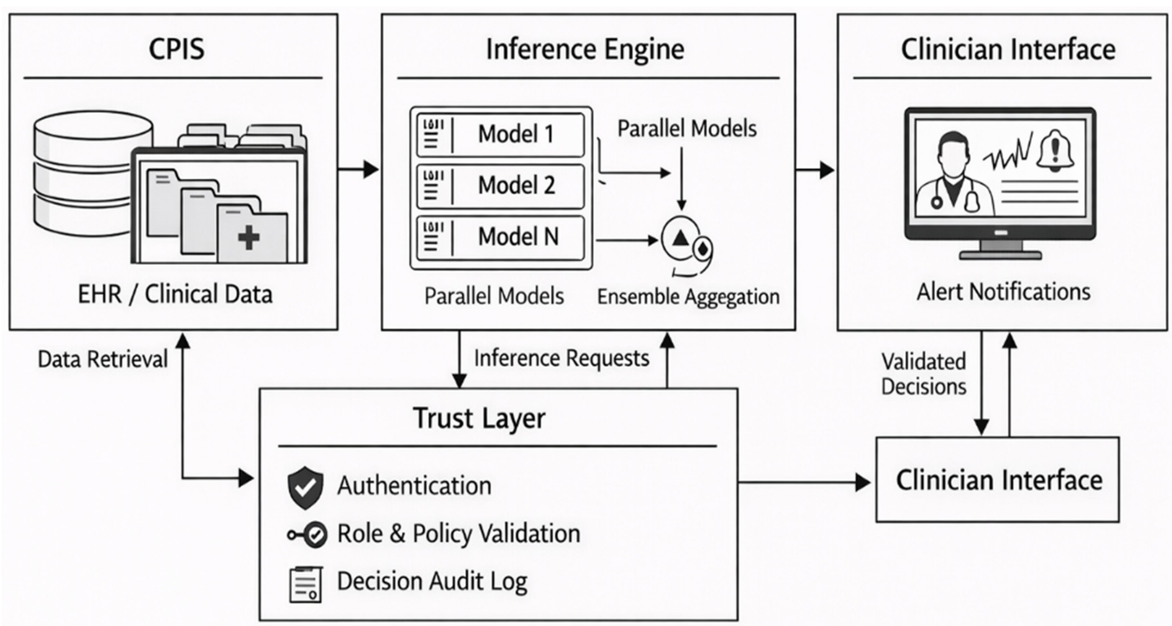

Figure 3: System architecture with inference engine, trust layer, and clinician interface

4. RESULTS

Experiments were conducted on a centralized EHR repository with dataset of identified patient records with multiple features. The clinical reasoning engine was implemented using tree-based Random Forest, XGBoost, which explores an ensemble aggregation with a constrained time-bound approach to ensure latency compliance. All models were evaluated in parallel, with latency tracing capturing inference time, aggregation delay, and trust enforcement overhead as in Table 2.

Table 2: Predictive Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score	AUC
Random Forest	0.91	0.92	0.90	0.91	0.95
XGBoost	0.93	0.94	0.91	0.92	0.96
Logistic Regression	0.87	0.88	0.85	0.86	0.90
Naive Bayes	0.84	0.85	0.82	0.83	0.88
Ensemble Aggregation	0.95	0.96	0.93	0.94	0.97

The ensemble model outperforms individual learners, achieving higher accuracy and AUC, indicating robust risk estimation under heterogeneous clinical data.

Table 3: Latency and Trust Overhead

Stage	Avg Latency (ms)
Data Ingestion	15
Model Inference (parallel)	120
Ensemble Aggregation	20
Trust Enforcement	10
Total End-to-End Latency	165

The total latency remains under clinically acceptable thresholds (~200ms), demonstrating the feasibility of real-time decision support with trust constraints.

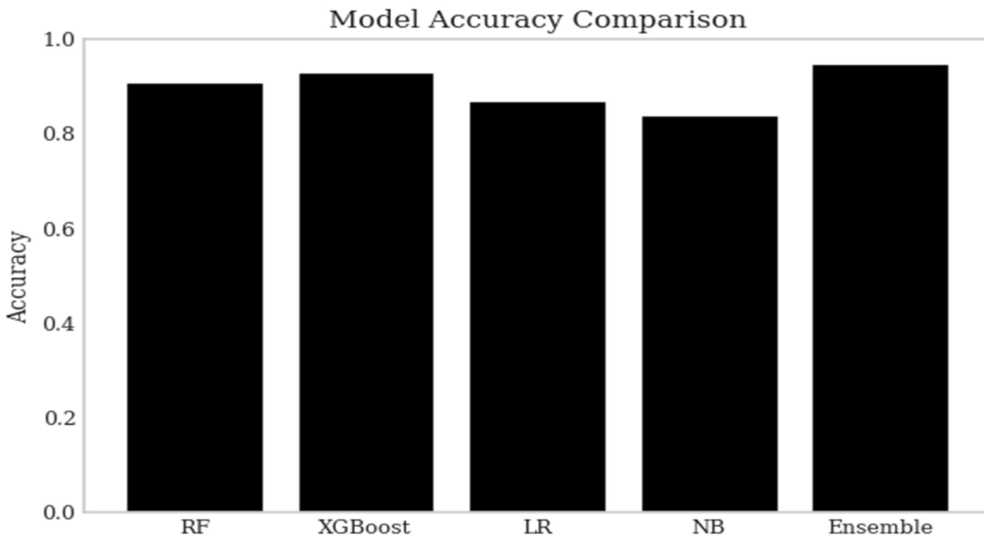

Figure 4: Model Accuracy Comparison

The bar chart demonstrates that the ensemble aggregation achieves the highest accuracy (0.95) compared to individual learners (RF: 0.91, XGBoost: 0.93). This confirms that combining multiple models mitigates the weaknesses of single models and improves robustness against heterogeneous and noisy clinical features. In practice, higher accuracy reduces misdiagnoses and enhances trust in automated alerts, ensuring clinicians can rely on the system for critical decision-making.

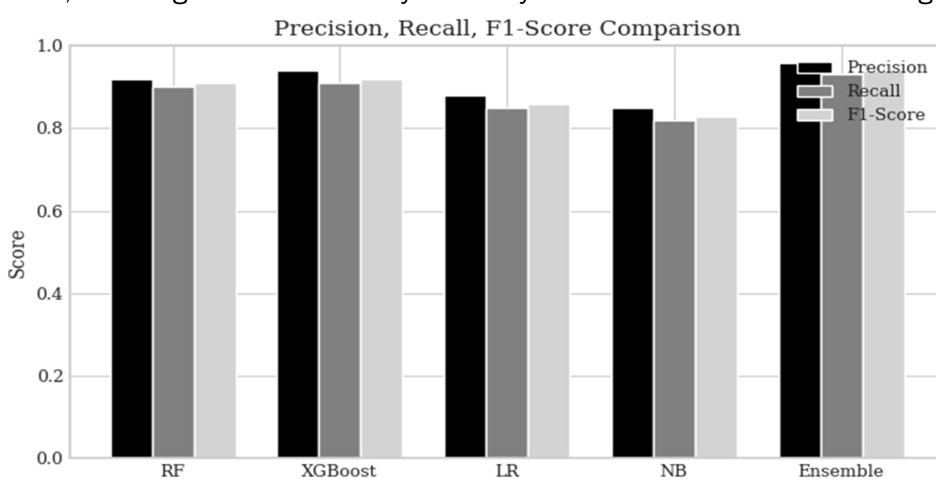

Figure 5: Precision, Recall, F1-Score Comparison

The multi-bar graph highlights that the ensemble maintains a high balance across precision (0.96) and recall (0.93), yielding an F1-score of 0.94. This indicates that the model effectively minimizes both false positives and false negatives, which is crucial for clinical applications where either type of error could compromise patient safety. The ensemble's balanced performance ensures consistent detection of at-risk patients while reducing unnecessary alerts.

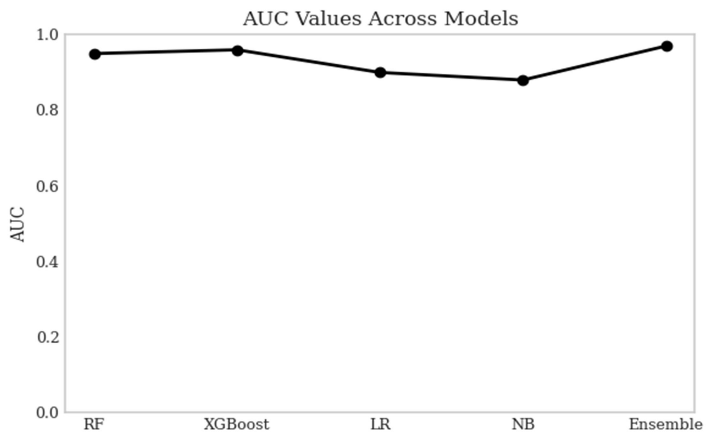

Figure 6: AUC Values Across Models

The line graph shows the ensemble attaining the highest AUC (0.97), indicating superior discrimination between positive and negative cases. A higher AUC translates to better risk stratification, allowing clinicians to prioritize interventions for high-risk patients. This result implies that the collective inference strategy captures complex feature interactions more effectively than individual models (Ojugo, Odiakaose, Emordi, Ako, et al., 2023; Ojugo, Yoro, et al., 2015).

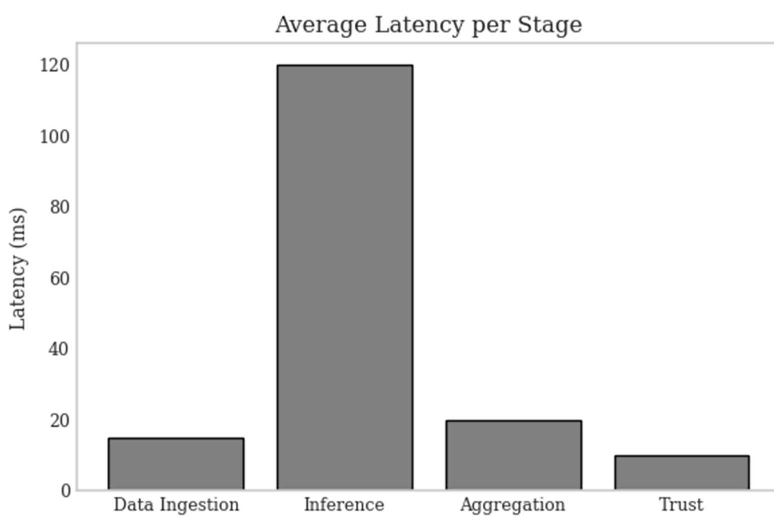

Figure 7: Average Latency per Stage

This bar chart shows that inference accounts for the largest portion of end-to-end latency (120 ms), while data ingestion, aggregation, and trust enforcement contribute minimally. The total latency (~165 ms) remains below the clinically acceptable threshold, confirming that the framework can deliver real-time recommendations without compromising patient care workflows.

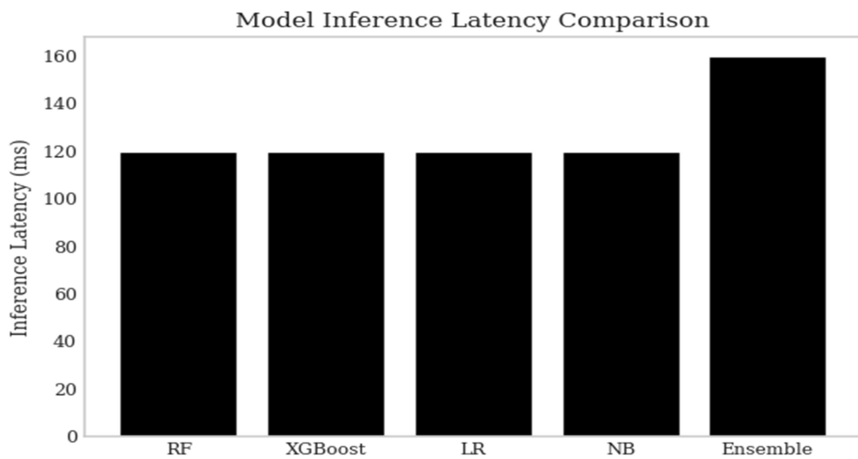

Figure 8: Model Inference Latency Comparison

The comparison illustrates that ensemble aggregation introduces only a slight increase in inference latency relative to single models. Despite this marginal increase, the improved predictive accuracy and trust-constrained decision guarantees justify the trade-off. This suggests that the system is operationally feasible and can scale to real-time clinical environments without excessive computational burden (Uddin et al., 2021).

5. DISCUSSION

The experimental evaluation demonstrates that the proposed trust-constrained clinical decision support system (CDSS) achieves a balance between predictive performance, operational efficiency, and governance compliance within a centralized healthcare infrastructure. By integrating parallel ensemble inference, latency-aware aggregation, and trust enforcement, the system delivers actionable recommendations that are both accurate and auditable, aligning with the requirements of modern healthcare environ. The predictive performance analysis reveals that the ensemble aggregation consistently outperforms individual models. The ensemble achieved Accuracy of 0.95, surpassing Random Forest (0.91) and XGBoost (0.93) – and aligns with previous studies to show that ensemble schemes enhance robustness via predictive patterns across heterogeneous clinical data (Onoma, Ugbotu, Aghaunor, Agboi, et al., 2025; Ugbotu, Emordi, et al., 2025).

Misclassifications that result in higher accuracy directly impact patient outcomes. Thus, ensemble maintained strong balance between precision (0.96) and recall (0.93) with F1-score of 0.94. Its high F1 indicates its successfully classified all benign data to minimize overfit, and ensuring high-risk patients are correctly identified (Eboka, Aghware, et al., 2025; Eboka, Odiakaose, et al., 2025). Our AUC of 0.97 confirms the ensemble's discriminatory ability to support robust risk stratification and informed clinical decision-making (Ejeh et al., 2024; Kim et al., 2022).

This result affirms that ensembles provide epistemic risk management, reduces reliance on any single model assumption while improving overall predictive reliability. Operationally, the latency analysis confirms that the system supports real-time decision support. Also, it dominates total end-to-end latency (120 ms), while data ingestion, aggregation, and trust enforcement contribute minimally, resulting in a total latency of approximately 165 ms.

This is well within clinically acceptable thresholds for timely alerts, indicating that the architecture can be deployed in high-paced clinical workflows without disrupting care delivery (Ojugo, Ejeh, Akazue, Ashioba, Odiakaose, et al., 2023; Ojugo & Ekurume, 2021). Also, the slight increase in latency by ensemble aggregation is outweighed by the gains in predictive robustness and governance compliance, confirming that the trade-off is operationally acceptable.

Our trust-constrained design differentiates this CDSS from conventional systems – and addresses known issues in CDSS deployments, where unregulated outputs compromise clinician trust. Attaching provenance metadata institutions demonstrate accountability in automated decision-making. The modular architecture further enhances reproducibility and extensibility. Model inference is decoupled from user context, ensuring consistent behavior across experiments. Parameterization of policy thresholds, timing limits, and model configurations allows adaptation to diverse clinical domains without extensive re-engineering, which is consistent with recommendations for scalable, interoperable healthcare systems (Amar et al., 2024; Kumar et al., 2024). This separation of concerns between intelligence and governance ensures that predictive robustness and trust enforcement can evolve independently, a key requirement in modern CDSS design.

6. CONCLUSION

The study demonstrated that meaningful clinical intelligence in centralized healthcare environments must be approached not as a purely algorithmic undertaking but as an institutional process grounded in trust, governance, and operational feasibility. By integrating model inference within a policy-aware centralized architecture, the proposed solution argues convincingly that accuracy alone cannot guarantee responsible decision support; instead, computational reasoning needs to be embedded within a context that verifies who requests intelligence, how it is generated, and under what authority actionable outputs are exposed. The framework's layered pipeline spanning clinical data ingestion, parallel model execution, aggregation under time constraints, and trust-conditioned emission provides a concrete pathway for reconciling predictive value with safety, auditability, and institutional accountability. The work advances the discourse on CDSS deployment by demonstrating that latency-bounded collective inference can match the realities of high-pressure clinical workflows without sacrificing model diversity or interpretive robustness. At the same time, the emphasis on provenance, traceability, and user-role verification responds to persistent concerns about clinician trust in automated systems, exposing how governance must be engineered into the computational fabric rather than appended post hoc as external compliance checks.

Taken together, the findings reinforce a larger conceptual shift in healthcare AI: from viewing machine learning as a “black box oracle” to understanding it as a controllable, auditable contributor within a larger clinical system whose legitimacy depends on policy enforcement as much as predictive performance. While the design presented here delivers a coherent path to safe deployment, it also highlights research directions worth pursuing, including extending trust validation across organizational boundaries, stress-testing ensemble behavior under multi-site variability, and integrating adaptive policies that reflect shifting clinical or public-health priorities. Ultimately, the proposed architecture underscores that trustworthy CDSS systems are socio-technical artifacts combining models, datasets, roles, institutional policies, and clinician interpretation and that durable adoption will depend on sustaining all of these elements in concert rather than privileging computational novelty alone.

REFERENCES

Abdulmalik, H. A., & Yassin, A. A. (2023). Secure two-factor mutual authentication scheme using shared image in medical healthcare environment. *Bulletin of Electrical Engineering and Informatics*, *12*(4), 2474–2483. https://doi.org/10.11591/eei.v12i4.4459

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

Aghaunor, T. C., Ugbotu, E. V., Ugboh, E., Onoma, P. A., Emordi, F. U., Ojugo, A. A., Geteloma, V. O., Idama, R. O., & Ezzeh, P. O. (2026). Investigating Security Enhancement in Hybrid Clouds via a Blockchain-Fused Privacy Preservation Strategy: Pilot Study. *Journal of Computing Theories and Applications*, *3*(4), 428–442. https://doi.org/10.62411/jcta.15508

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., Ojugo, A. A., Adigwe, W., Odiakaose, C. C., Ojei, E. O., Ashioba, N. C., Okpor, M. D., & Geteloma, V. O. (2024). Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection. *Journal of Computing Theories and Applications*, *1*(4), 407–420. https://doi.org/10.62411/jcta.10323

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. doi: 10.11591/ijict.v13i2.pp178-187

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023). 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

Agrafiotis, I., Nurse, J. R., Buckley, O., Legg, P., Creese, S., & Goldsmith, M. (2015). Identifying attack patterns for insider threat detection. *Computer Fraud and Security*, *2015*(7), 9–17. https://doi.org/10.1016/S1361-3723(15)30066-X

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., 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

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. doi: 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

Allenotor, D., & Ojugo, A. A. (2017). A Financial Option Based Price and Risk Management Model for Pricing Electrical Energy in Nigeria. *Advances in Multidisciplinary & Scientific Research Journal*, *3*(2), 79–90.

Allenotor, D., Oyemade, D. A., & Ojugo, A. A. (2015). A Financial Option Model for Pricing Cloud Computational Resources Based on Cloud Trace Characterization. *African Journal of Computing & ICT*, *8*(2), 83–92. www.ajocict.net

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

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

Binitie, A. P., Onyemenem, S. I., Anujeonye, N. C., Adimabua, A., Egbokhare, F. A., & Aghaunor, T. C. (2026). A Graph-Augmented Isolation Forest Using Node2Vec and GraphSAGE for Mobile User Behavior Anomaly Detection. *Journal of Computing Theories and Applications*, *3*(3), 369–383. https://doi.org/10.62411/jcta.15494

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

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

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11), 341. https://doi.org/10.3390/fi14110341

Hakonen, P. (2022). Detecting Insider Threats Using User and Entity Behavior Analytics. *International Journal of Electrical and Computer Engineering*, *21*(October), 5765–5783. https://www.theseus.fi/handle/10024/786079

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. *Journal of the Nigerian Society of Physical Sciences*, *5*(2), 992. https://doi.org/10.46481/jnsps.2023.992

Ibrahim, T., & Ali, H. (2023). The Impact of Wearable IoT Devices on Early Disease Detection and Prevention. *International Journal of Applied Health Care Analytics*, *8*(8), 1–15. https://norislab.com/index.php/IJAHA/article/view/27

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

Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B., & Raza, U. (2021). Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia Systems*, *27*(4), 787–806. https://doi.org/10.1007/s00530-020-00687-0

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*. doi.org/10.1587/trans.E0.

Kim, J. W., Kim, S. J., Cha, W. C., & Kim, T. (2022). A Blockchain-Applied Personal Health Record Application: Development and User Experience. *Applied Sciences*, *12*(4), 1847. doi: 10.3390/app12041847

Li, W., Laghari, S. U. A., Manickam, S., Chong, Y. W., & Li, B. (2024). Machine Learning-Enabled Attacks on Anti-Phishing Blacklists. *IEEE Access*, *12*(December), 191586–191602. https://doi.org/10.1109/ACCESS.2024.3516754

Li, W., Manickam, S., Chong, Y., & Karuppayah, S. (2025). *Talking Like a Phisher: LLM-Based Attacks on Voice Phishing Classifiers*. *July*. https://doi.org/10.48550/arXiv.2507.16291

Lötsch, J., Mustonen, L., Harno, H., & Kalso, E. (2022). Machine-Learning Analysis of Serum Proteomics in Neuropathic Pain after Nerve Injury in Breast Cancer Surgery Points at Chemokine Signaling via SIRT2 Regulation. *International Journal of Molecular Sciences*, *23*(7). https://doi.org/10.3390/ijms23073488

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., 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

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

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a User-Trust Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study. *Journal of Computing Theories and Applications*, *1*(2), 50–60. https://doi.org/10.33633/jcta.v1i2.9259

Ojugo, A. A., Allenotor, D., Oyemade, D. A., Yoro, R. E., & Anujeonye, C. N. (2015). Immunization Model for Ebola Virus in Rural Sierra-Leone. *African Journal of Computing & ICT*, *8*(1), 1–10.

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. (2019). 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. (2021a). Forging a Spectral-Clustering Multi-Agent Hybrid Deep Learning Model To Predict Rainfall Runoff In Nigeria. *International Journal of Innovative Science, Engineering and Technology*, *8*(3), 140–147.

Ojugo, A. A., & Nwankwo, O. (2021b). Multi-Agent Bayesian Framework For Parametric Selection In The Detection And Diagnosis of Tuberculosis Contagion In Nigeria. *JINAV: Journal of Information and Visualization*, *2*(2), 69–76. https://doi.org/10.35877/454ri.jinav375

Ojugo, A. A., & Nwankwo, O. (2021c). 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. (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. doi: 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. (2020). Predicting Futures Price And Contract Portfolios Using The ARIMA Model : A Case of Nigeria ' s Bonny Light and Forcados. *Quantitative Economics and Management Studies*, *1*(4), 237–248. https://doi.org/10.35877/454RI.qems139

Ojugo, A. A., Yoro, R. E., Eboka, A. O., Yerokun, M. O., Anujeonye, C. N., & Efozia, F. N. (2015). Predicting Behavioural Evolution on a Graph-Based Model. *Advances in Networks*, *3*(2), 8. https://doi.org/10.11648/j.net.20150302.11

Okeke, K., & Omojola, S. (2025). Enhancing Cybersecurity Measures in Critical Infrastructure: Challenges and Innovations for Resilience. *Journal of Scientific Research and Reports*, *31*(2), 474–484. https://doi.org/10.9734/jsrr/2025/v31i22868

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. doi.org/10.62411/faith.2024-14

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

Olaniyi, O. O., Okunleye, O. J., Olabanji, S. O., Asonze, C. U., & Ajayi, S. A. (2023). IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience. *Asian Journal of Research in Computer Science*, *16*(4), 354–371. https://doi.org/10.9734/ajrcos/2023/v16i4397

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. (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

Palanisamy, V., & Thirunavukarasu, R. (2019). Implications of big data analytics in developing healthcare frameworks – A review. *Journal of King Saud University - Computer and Information Sciences*, *31*(4), 415–425. https://doi.org/10.1016/j.jksuci.2017.12.007

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, *7*(2), 229–233. https://doi.org/10.1016/j.icte.2020.09.002

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.

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

San, K. K., Win, H. H., & Chaw, K. E. E. (2025). Enhancing Hybrid Course Recommendation with Weighted Voting Ensemble Learning. *Journal of Future Artificial Intelligence and Technologies*, *1*(4), 337–347. https://doi.org/10.62411/faith.3048-3719-55

Setiadi, D. R. I. M., Muslikh, A. R., Iriananda, 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. (2025). 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. doi: 10.32604/cmc.2025.063729

Sheikhtaheri, A., & Sabermahani, F. (2022). Applications and Outcomes of Internet of Things for Patients with Alzheimer's Disease/Dementia: A Scoping Review. *BioMed Research International*, *2022*(1). https://doi.org/10.1155/2022/6274185

Sheng, W. J., Kasmin, I. F., Amin, S., & Zainal, N. K. (2023). Addressing user perception and implementing Hedera Hashgraph and voice recognition into Multi-Factor Authentication (MFA) system. *International Journal of Data Science and Advanced Analytics*, *4*, 194–201. https://doi.org/10.69511/ijdsaa.v4i0.165

Sun, Y., & Gu, L. (2021). Attention-based Machine Learning Model for Smart Contract Vulnerability Detection. *Journal of Physics: 1820*(1), 012004. doi: 10.1088/1742-6596/1820/1/012004

Tahir, H. T., Aghaunor, T. C., Ugbotu, E. V., Onoma, P. A., Ojugo, A. A., Abere, R. A., Agboi, J., & Aherobo, V. O. (2025). Enhancing Security with Blockchain-Enabled Privacy Preservation for Multi-and-Hybrid Cloud Environment: A Pilot Study. *Advances in Multidisciplinary & Scientific Research Journal Publication*, *16*(4), 25–44. https://doi.org/10.22624/AIMS/CISDI/V16N4P3

Uddin, M., Salah, K., Jayaraman, R., Pesic, S., & Ellahham, S. (2021). Blockchain for drug traceability: Architectures and open challenges. *Health Informatics Journal*, *27*(2), 146045822110112. https://doi.org/10.1177/14604582211011228

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., Ako, R. E., Odoh, A., Oghorodi, D., Okpako, A. E., Aghaunor, T. C., Emordi, F. U., Ugboh, E., Agboi, J., Odiakaose, C. C., Ojugo, A. A., Geteloma, V. O., Abere, R. A., Idama, R. O., Eboka, A. O., Ezzeh, P. O., Onochie, C. C., Oweimieotu, A. E., Ojo, B., & Onoma, P. A. (2025). Equipping the GREDDIoMT Device with Early Behavioural Risk Detection of Dementia via a Pre-Activated SENet fused BiGRU. *Journal of Behavioral Informatics, Digital Humanities and Development Research*, *11*(3), 36–56. https://doi.org/10.22624/AIMS/BHI/V11N3P4

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.

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

Zhang, X., Wang, Q., Li, R., & Wang, Q. (2022). Frontrunning Block Attack in PoA Clique: A Case Study. *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022*, 1–7. https://doi.org/10.1109/ICBC54727.2022.9805543

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