American Journal of
Strategic Studies
(AJSS)

A Privacy-Preserving Federated Data Exchange Architecture for Trusted Cross-Border Digital Services in the East African Community

American Journal of Strategic Studies
ISSN: 2790-6191 (Online)
Vol. 8, Issue No. 1, pp 83 – 104, 2026
www.carijournals.org

A Privacy-Preserving Federated Data Exchange Architecture for Trusted Cross-Border Digital Services in the East African Community

Abdinasir Ismael Hashi*[1], Osman Abdullahi Jama[2]

[1, 2,] Computer Science, Somali National university, Mogadishu, Somalia

https://orcid.org/0009-0009-0635-2609

Accepted: 22nd August, 2026, Received in Revised Form: 8th September, 2026, Published: 22nd September, 2026

Abstract

Purpose: Cross-border digital services are growing rapidly in the East African Community (EAC), with higher demand for secure, trustworthy data exchange and safeguarding of institutions' data ownership and privacy. Given these issues, this paper presents a Privacy-Preserving Federated Data Exchange Architecture (PP-FDEA).

Methodology: The architecture integrates federated learning, decentralized data control, authentication, authorization, consent management, encryption and differential privacy, as well as auditable governance. Country Health Indicators data is distributed across virtual EAC nodes representing Kenya, Uganda and Tanzania to evaluate the proposed architecture. The data used for training are stored locally and the number of samples is about 775–780 per node and the distribution does not change even by 5 samples.

Findings: The Multi-Round FedAvg achieves an independent-test accuracy of about 0.82 and a DP-FedAvg with noise multiplier 0.3 achieves an independent-test accuracy of 0.80. Latency is still low, between 0.50 and 0.61ms, while all five governance and security scenarios get a score of 100%.

Unique Contribution to Theory, Practice and Policy: Overall, the results show the potential of PP-FDEA for providing secure, privacy preserving, scalable and trusted EAC cross-border digital services.

Keywords: *Federated Learning; Differential Privacy; Cross-Border Data Exchange; Data Sovereignty; East African Community (EAC).*

1. Introduction

New developments in digital public infrastructure, eID, mobile financial services, digital health, e-government and cross-border trade are revolutionizing service delivery in the East African Community (EAC) [1]. In an era of increasingly entangled regional economies, the availability of trustworthy exchanges of personal, financial, administration and transactional data across borders is vital to interoperable digital services [2]. But traditional architectures of central data sharing raise a number of concerns – both in relation to privacy, data sovereignty, unauthorised access, regulatory fragmentation and institutional trust [3]. The problems are especially significant in the EAC region where the member states have different legal, technological, organizational and cyber security systems and frameworks [4]. The federated data exchange architecture approach may help to resolve these problems by allowing local authorities to have full ownership of the data and using secure, auditable and interoperable structures to share only authorized data [5-7].

While there have been significant efforts to improve privacy, as well as the implementation of federated identity, distributed systems, privacy-preserving technologies and secure data-sharing protocols, many these approaches still deliver the fragmented solutions that fail to meet privacy preservation, cross-border interoperability, trust management, consent, accountability and regulatory compliance at the same time [8-10]. Lack of a regionally acceptable framework would create higher exposure risks of data and limit the growth of the development of seamless digital services in member states of the EAC [11]. Hence, a conceptual solution for Privacy-Preserving Federated Data Exchange Architecture (PP-FDEA) is proposed that integrates federated governance, decentralized data control, robust authentication and encryption, data access consent, privacy-enhancing mechanisms, trusted transaction log and policy-based interoperability [12-14] . This architecture could provide a secure way to exchange information without needless centralization of sensitive data and thus help to reinforce the privacy of users, the autonomy of institutions and the trust in area digital services. The objectives of this study are to:

i. To develop a privacy-preserving federated data exchange architecture that enables secure and controlled cross-border data sharing while retaining data sovereignty within participating EAC institutions and jurisdictions.

ii. To design a trusted interoperability and access-control framework integrating federated identity, authentication, authorization, consent management, encryption and policy enforcement for secure digital-service transactions.

iii. To establish privacy, trust and accountability mechanisms using privacy-enhancing technologies, auditable transaction records, data-minimization principles and risk-aware governance for cross-border information exchange.

iv. To evaluate the proposed architecture in terms of privacy protection, security, interoperability, latency, scalability, trustworthiness and service efficiency under representative EAC cross-border digital-service scenarios.

American Journal of Strategic Studies
ISSN: 2790-6191 (Online)
Vol. 8, Issue No. 1, pp 83 – 104, 2026
www.carijournals.org

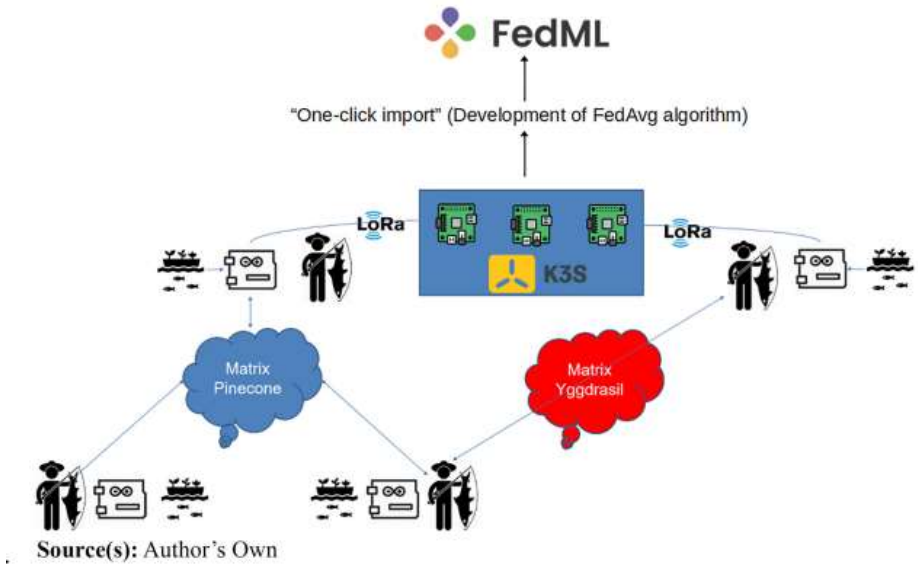


Figure 1: System architecture: FL algorithm layer: FedML open platform [15]

The rest of the paper is organized as follows. Section 2 provides an overview of the literature where the concept of federated data exchange, privacy-preserving computing, digital identity, cross-border interoperability, cybersecurity and trusted digital services were explored and the key study gaps pertinent to the EAC environment were identified. The problem, the requirements of the system, assumptions taken, the threat model and the design principles that guided the design of the proposed architecture are introduced in Section 3. In Section 4, the proposed privacy-preserving federated data exchange architecture is introduced which consists of federated nodes, identity and trust layer, consent and policy-management layer, secure communication layer, privacy-preserving components and audit framework. The methodological and evaluation framework are described in Section 5 for the evaluation of security, privacy, interoperability, computational overhead, communication latency, scalability and reliability. The results of the evaluation are presented and discussed in section 6 in comparison with conventional and centralized approaches to data exchange. The implications for trusted cross-border digital services, data sovereignty, institutional governance and regional digital integration are discussed in section 7. Finally, in Section 8, the work is concluded and future study directions such as real-world pilot deployment, advanced privacy-enhancing technologies, AI-assisted trust management and adaptive regulatory-policy enforcement across EAC member states are highlighted.

2. Literature Review

In recent years, a significant amount of study has been directed towards privacy-preserving federated architectures in the cross-border provision of services in healthcare and information technology. Zhang et al., 2026 [16] used the XACML access control model to provide attribute-based access control (ABAC) and proposed FLA3, which operates authentication, authorization and accounting (AAA) based on XACML, cryptographic accounting and study-scoped federation. Evaluation showed that the model's predictive performance was on par

with centralized learning and it was deployed at 5 institutions in 4 countries and evaluated on 54,446 samples from 35,315 subjects from 25 evaluation centres, all while maintaining governance constraints. Likewise, with regard to cross-sectional telemedicine models, Meyo and colleagues designed a FL model based on synthetic EHRs across 7 hospitals in the three nations of Kenya, Tanzania and Uganda [17]. Increased the accuracy by 0.0665, recall by 0.1193 and F1 by 0.0657 compared to centralized training. Under centralized learning, the success rate for the model-inversion attack was 0.696, whereas it was reduced to 0.638, which was a decrease of 8.4%, with the membership-inference leakage around the AUC of 0.50. Regarding interoperability needs for Foundational Identity Systems in the African digital identity domain, Ibor et al. (2025) [18] discussed several challenges, including data sovereignty, institutional trust, vendor lock-in, system compatibility and incomplete legislation. It compare eIDAS and Estonian X-Road and show the relevance of interoperability of identity and authentication mechanisms for cross-border digital government services.

In addition to health and identity, researchers have explored privacy, governance, cybersecurity and digital trade as related facets of the cross-border flow of data. For the heterogeneous FL, Lin et al. 2025 [19] proposed a FL system that integrates differential privacy (DP), partial homomorphic encryption (PHE), blockchain and automated regulatory governance. It guaranteed a data-protection integrity of 97.3% and a prediction accuracy of 89.4% with 12.8 million cross-border transactions, while minimizing privacy leakage from 15.1% to 1.9% ($p<0.001$). It also successfully cleared through 83.6% of simulated ethical conflicts and minimized free-riding by 67.2% with governance latency of 162 ms at 10,000 TPS. Sarhan et al. (2023) [20] suggested an SDPA that uses a decentralized Private Set Intersection process with an average CPU-based processing time of about 775 ms which was much less than that of the ADB-SMC with an average CPU-based processing time of 900 ms. In the EAC region, Joseph et al. (2026) [21] found that trust deficiencies, interoperability issues, infrastructure limitations, sovereignty concerns and legal fragmentation were significant challenges to cyber-threat-intelligence sharing between Kenya, Uganda and Tanzania. Okwor et al., 2026 [22] also noted that 76.5% of the experts identified regional blocs as being very important to AI governance and 67.6% identified capacity gaps as not enough technical, legal, or institutional capacity. These results all point toward the need to strengthen the effectiveness of the technical mechanisms for protecting privacy and security with enforceable regional governance and trust mechanisms.

In terms of cross-border services, study on digital trade in Africa further stresses the importance of infrastructure, regulatory harmonization and institutional readiness. A conceptual model that connects the concepts of cross-cultural adaptation, green marketing and inclusive business-model innovation through digital platforms and FinTech was developed by Ebabu et al. (2026) [23]. However, African cross-border trading in e-commerce continues to be hindered due to digital divides, logistics inefficiencies, trust issues and regulatory fragmentation, as highlighted by Sampson et al. (2025) [24]. In a study of 94 Rwandan women entrepreneurs, Mutesi et al. (2025) [25] highlighted limited literacy to

digital technologies, technology adoption and awareness of the AfCFTA regulations as key challenges. The same was found by Olalekan et al. (2024) in the African context where regulatory fragmentation and infrastructure deficits and cyber security risk were also identified as hindrances to the functioning of African Cross-Border Payment Systems. Panga et al. (2024) [27], based on 376 respondents, found significant effects of one-stop border posts (β=0.636), coordinated agencies (β=0.261), trade facilitation (β=0.245) and customs harmonization (β=0.211) on logistics performance. Building digital connectivity and policy harmonisation were also found by Ahmed et al. (2024) [28] to challenge regional integration. Subramanian et al. [29] showed privacy-preserving identity access and identity-based attribute access control in the federated cloud. More recently, Abraham et al. (2026) [30] proposed AfriPShare, which was based on FL and Local Differential Privacy that achieves accuracy of 94.3% ± 0.6% on ε=1.0. Huang et al. (2026) [31] proposed FedPrivGov for prediction tasks across organizations in the field of public health and achieved a 7% improvement in accuracy (from 74.3% to 81.2%) and 77% improvement in AUC (0.761 to 0.833), with only about 1% loss under privacy constraints. Taken together, these studies show that current solutions focus primarily on privacy, interoperability, governance, or digital infrastructure, but do not consider them in relation to each other. The architecture of a coordinated exchange of federated data with emphasis on trusted, sovereign and interoperable cross-border digital services in the EAC has still not been developed to a level sufficient enough to handle data exchange.

3. Research Methodology

The study follows a design-science and experimental study approach to design and assess federated data exchange architecture with privacy protection for trusted cross-border digital services in the EAC. The methodology was based on the idea that the base paper, which was to have the sensitive data remain within participating institutions and have the governance and security controls placed in the orchestration layer of the federation. The architecture in the base paper was a separation of coordination, local gateway functions and execution of the studies, with institutional data sovereignty.

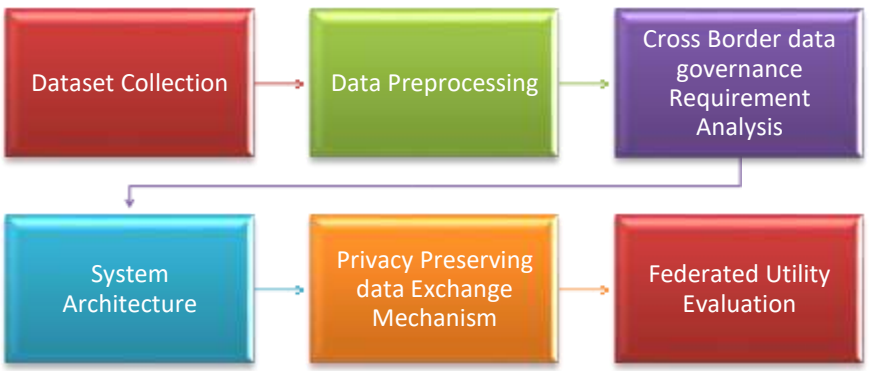


Figure 2: Framework of the Methodology

3.1 Dataset Collection

The dataset was the Country Health Indicators dataset [33], which was a public dataset and could be used to simulate cross-border federated data exchange. The data was compiled from a variety of open sources, such as COVID-19 cases and deaths, cause of death, food sources, health care systems, vaccination status, school closures and socioeconomic indicators. In the suggested architecture of the EAC, it was proposed that the architecturally defined EAC Country-level records are partitioned to individual virtual institutional nodes representing the participating entity states of EAC. All records are kept locally stored and only updates to the models (which do not expose private information) or aggregated information are shared.

3.2 Data Preprocessing

Each participating EAC institution preprocesses the data prior to federated computation. All of the raw data items are subject to the control of institutions throughout the cleaning, normalization and transformation of features. The procedures involve data quality enhancement, data consistency and exchange of only processed model representations/represents or outputs authorized by the federation coordinator which ensures data privacy and data sovereignty.

$$D_i' = \text{Preprocess}\ (D_i) \tag{1}$$

- **Data Cleaning**

Before the federated learning process, local data cleaning processes are applied to eliminate, correct or update invalid/duplicated/incomplete/inconsistent records. No raw data was shared externally; each institution has its own set of quality rules to apply to its data. This process increases reliability and consistency of participating datasets and maintains institutional ownership and confidentiality of sensitive cross-border information.

$$D_i' = \text{Clean}\ (D_i) \tag{2}$$

$$D_i' = \{x \in D_i |\ \text{Valid}(X) = 1\} \tag{3}$$

- **Data Normalization**

It normalizes the numerical attributes locally to decrease differences in scale across institutional data sets. Min–max normalization scales each feature to a known range, usually [0, 1]. Normalization prior to model training helps to improve numerical stability, facilitates an effective optimization and avoids high magnitude attributes dominating the federated learning results.

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{4}$$

$$0 \leq x' \leq 1 \tag{5}$$

- **Local Feature Transformation**

Feature transformation was locally applied to transform the attributes of each institution to appropriate representations for the federated model training. The transformation could be

encoding, dimensionality reduction or feature extraction. The processing takes place before the communication step; sensitive raw features stay inside the institutions, reducing the exposure and enabling the creation of uniform inputs for the computation processing that takes place across institutions.

$$x_i' = f(X_i) \tag{6}$$

$$X_i \nrightarrow \text{Coordinator} \tag{7}$$

3.3 Cross-Border Data Governance Requirement Analysis

The proposed data governance framework for cross-border data exchange assures trust and proper authorization of the EAC institutions involved in data exchange [34]. The federation was secured by a registered identity of the institutions established with a digital certificate which ensures protection of the federation from unauthorized entry. The authentication decision was defined as:

$$\text{AuthID}(n) = \begin{cases} 1, & \text{Cert}(n) \in \text{TrustRegistry} \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

The (Cert(n)) symbol stands for the participant certificate and the (TrustRegistry) symbol was for the trusted EAC institutional registry. The services are also authorized in a service-scoped manner:

$$\text{ServiceAuth}(n,s) = \begin{cases} 1, & n \in \text{Members}(s) \\ 0, & n \notin \text{Members}(s) \end{cases} \tag{9}$$

Role based least-privilege access restricts operations as per the role assigned:

$$\text{RoleAuth}(n,a) = \begin{cases} 1, & \text{Role}(n) \in \text{Allowed}(a) \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

Temporal validity means that the authorization would only be accepted before the expiration of the service:

$$v_s(s, t) = \begin{cases} 1, & t < \text{Expiry}(s) \\ 0, & t \geq \text{Expiry}(s) \end{cases} \tag{11}$$

The combination of the two authorization conditions could then be written as follows:

$$\text{Access}(n,s,a,t)=\text{AuthID}(n)\times\text{ServiceAuth}(n,s)\times\text{RoleAuth}(n,a)\times Vs(s,t) \tag{12}$$

Thus, (Access=1) only when all governance conditions are satisfied; otherwise, access was denied. Finally, accountability was maintained through:

$$\text{AuditEvent}=(IDn, A, S, T, D, P) \tag{13}$$

Maintaining traceability of all Cross-Border operations involving security.

3.4 System Architecture of the Proposed EAC Federated Data Exchange

The proposed architecture consists of **three principal layers**, adapted from the base paper's three-layer federated architecture [35]. The base paper uses central coordination, site-local gateways and isolated application processes to preserve institutional data sovereignty.

- **Central Federation Coordination Layer**

The entities participating to the Federation are managed from a central point by the EAC Federation Coordinator, the service registration, the Federation sessions, the policy distribution, the model updates, the aggregation, the trust and the auditing. Sensitive data was kept in the institution, thus eliminating the possibility of centralized data exposure [36]. During federation operations, the coordinator was responsible for only authorised metadata, policies and model parameters.

$$\text{RawDataCoordinator}=0 \tag{14}$$

- **Member-State Gateway Layer**

Every EAC institution has a local gateway that handles federated learning, security functions, data and policy management in a secure way [37]. The gateway provides institutional control on sensitive information with federal coordination control of communication. No raw data leaves the institution, enabling the sharing of data across the nations while preserving privacy and controlled participation.

$$G_i = \{ DB_i , PEP_i , FL_i , SEC_i \} \tag{15}$$

$$\text{RawData}_i \nrightarrow \text{Coordinator} \tag{16}$$

- **Local Data and Federated-Service Layer**

Highly sensitive data was kept in the originating EAC institution and would not be moved to a central location. Rather, the local systems update (or authorize query) model before secure exchange. This helps maintain institutional data sovereignty, limit risks of exposure and allows for privacy-preserving cross-border digital collaboration.

$$D_i \nrightarrow D_{central} \tag{17}$$

$$D_i \rightarrow \{ \text{Model}_i , \text{Query}_i \} \rightarrow \text{Secure Exchange} \tag{18}$$

- **Cross-Border Federated Data Exchange Model**

The EAC federation was made up of participating (K) institutions where (K) each has its own private data set locally. Institutions train the shared models independently, without sharing sensitive records with a central coordinator, but only sending updates to and from the models when it was authorized to do so [38]. In this architecture, it retains data sovereignty, minimizes exposure threats and allows for a collaborative shared intelligence using federated learning protocols, all while maintaining security and protection from exposure risks across borders.

$$N = \{ N_1 , N_2 , \ldots\ldots\ldots , N_K \} \tag{19}$$

$$D = \bigcup_{i=1}^{K} D_i , \; D_i \nrightarrow C \tag{20}$$

$$\theta_i^{i+1} = \text{Local Train } (D_i, \theta^t) \quad (21)$$

$$\text{Update}_i = \theta_i^{i+1} - \theta^t \quad (22)$$

3.5 Federated Learning Model

Proposed federated learning model – collaboratively training a global model without sharing raw data would be achieved by authorized EAC institutions. The local objective of minimizing the global objective was achieved for (K) participating institutions based on the size of local data sets:

$$\min_\theta F(\theta) = \sum_{i=1}^{K} \frac{n_i}{n} F_i(\theta) \quad (23)$$

$$N = \sum_{i=1}^{K} n_i \quad (24)$$

where (F_i (θ^t)) represents the local objective and (n_i) denotes the number of records at institution (i). Local training updates the model using gradient descent:

$$\theta_i^{i+1} = \theta^t - \eta \nabla F_i(\theta^t) \quad (25)$$

Only authorized institutions participate:

$$P_i = \{ i \in N \mid \text{Auth}(i,s,t) = 1 \} \quad (26)$$

The global model was then aggregated using weighted averaging:

$$\theta^{i+1} = \frac{n_i}{\sum_{j \in p_i} n_j} \theta_i^{i+1} \quad (27)$$

Thus, privacy was maintained while compliant institutions jointly improve model performance.

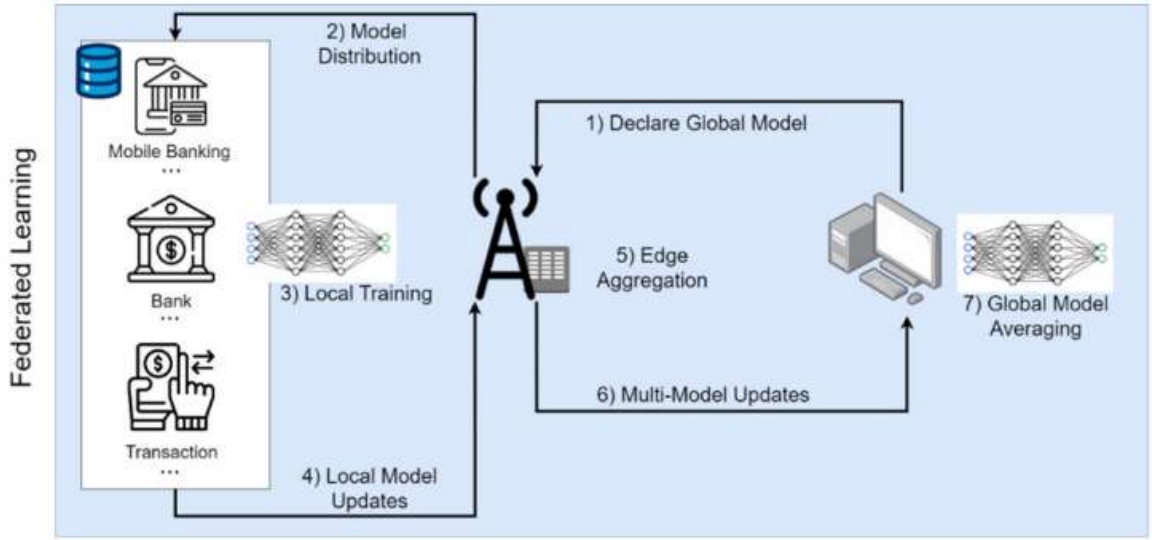


Figure 3: FL procedure flows in digital finance learning [39]

3.6 Privacy-Preserving Data Exchange Mechanism

Federated learning doesn't stop information leakage from model updates automatically. Thus, the proposed EAC architecture was based on the base framework with pre-transmission

differential privacy. Local gradients are also clipped to reduce sensitivity and then calibrated gaussian noise was added [40]. The resulting mechanism gives an (δ ,ϵ)-differential privacy guarantee. The lower the value of \epsilon, the stronger the privacy.

$$\bar{g_i} = \frac{g_i}{\max(1, ||g_i||2/C)} \tag{28}$$

$$\tilde{g_i} = \bar{g_i} + N(0, \sigma^2 C^2 I) \tag{29}$$

$$\text{Privacy} = (\delta, \epsilon) - \text{DP} \tag{30}$$

- **Authentication Mechanism**

Each participating institution would verify its institutional credentials and for access to the EAC, establish a trust relationship with the EAC in the proposed EAC architecture. Mutual TLS (mTLS) could ensure that each node was associated with the organization's identity without changing authentication and authorization. The identity structure could be verified across borders but does not reveal underlying datasets. Only after successfully performing a certificate and a trust check, would admission take place, making the federation more secure and accountable between participating institutions.

$$\text{Auth}(n_i) = \text{CertVerify}(\text{Cert}_i) \wedge \text{TrustVerify}(n_i) \tag{31}$$

$$\text{Auth}(n_i) = 1 \Longrightarrow \text{Admit}(n_i) \tag{32}$$

$$\text{Identity}_i = \{ \text{OrgID}_i, \text{Country}_i, \text{Service}_i, \text{Cert}_i \} \tag{33}$$

3.7 Cross-Border Communication Model

The presented EAC architecture was based on client-initiated communication, to enable institutions running behind a firewall or egress-only networks. Communication happens within each institution using their own gateway, thus minimizing inbound connectivity to institutional systems. This model provides better deployments compatibility and provides secure federation coordination at the same time. Performance of communication was measured using the following delay metrics: Authentication delay, Policy evaluation delay, Communication delay and Aggregation delay. Each federated exchange would have its own processing and transmission time, so the total latency would be the sum of all those timings.

$$\text{Institution}_i \rightarrow \text{Gateway}_i \rightarrow \text{EAC Coordinator} \tag{34}$$

3.8 Federated Utility Evaluation

The discovery of whether privacy and governance mechanisms maintain model performance was part of federated utility evaluation. The local processing, conventional federated learning, proposed privacy-preserving federated learning and centralized reference model are compared. The accuracy, precision, recall and f1 score are employed for assessing this. These metrics are quantitative proof of classification effectiveness and possible lost utility due to privacy-preserving controls in cross-border federated processing.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (35)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (36)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (37)$$

$$F1 = \frac{2\,(\text{Precision})(\text{Recall})}{\text{Precision}+\text{Recall}} \quad (38)$$

4. Results and Discussion

The results part measures the proposed privacy preserving federated data exchange architecture from various perspectives. It looks at the federated model convergence, predictive performance and performance at the local EAC node on Kenya, Uganda and Tanzania and distribution of training data. With increasing number of nodes participating in the communication, the efficiency of the communication was evaluated in terms of latency and scalability. The section also compares the performance of the different methods in terms of convergence and classification accuracy with the differential privacy (DP) and governance and security verification. All of the above prove the architecture's privacy, security, efficiency, scalability and trusted cross-border data-exchange capacities.

4.1 Federated Model Performance and Convergence

The figure 4 shows the convergence of the Federated Averaging (FedAvg) model for the proposed architecture of privacy-preserving data exchange over 5 federated rounds. The accuracy is initially at 0.6735 in Round 1, but drops to 0.6630 in Round 2 and then comes back up to 0.6658 in Rounds 3 and 4 and falls to 0.6615 in Round 5. Similarly, F1 decreases from 0.6650 to 0.6490 in Round 2, then rises to approximately 0.6533 in Rounds 3 and 4, followed by 0.6513 in Round 5. The performance level following Round 2 remains fairly steady suggesting a level of federated convergence across trusted digital services across borders.

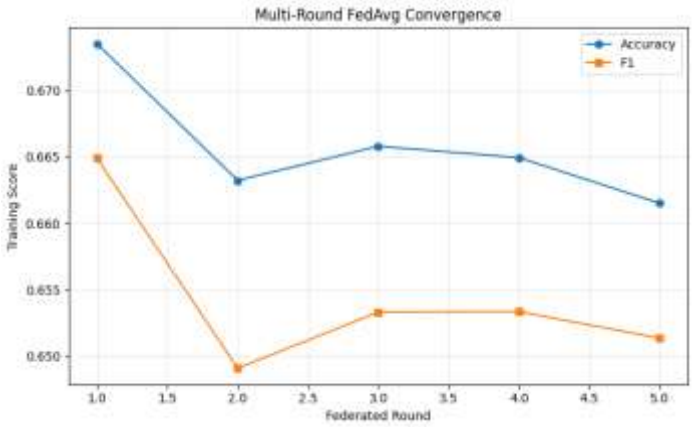


Figure 4: Multi-Round FedAvg Performance Convergence

Figure 5 shows the independent-test accuracy of three tested models for the suggested privacy preserving federated data exchange architecture. The HistGradientBoosting model is

the best predictor with accuracy around 0.94. The Multi-Round FedAvg model achieves an accuracy of ~0.82, demonstrating that the model achieves good performance in distributed learning with data locality. The DP-FedAvg (Noise=0.3) model achieves around 0.80 accuracy, where only around 0.02 of accuracy is affected by the introduction of DP. The outcomes of these results reveal the positive privacy protection, federated collaboration and predictive accuracy in trusted cross-border digital services in East Africa.

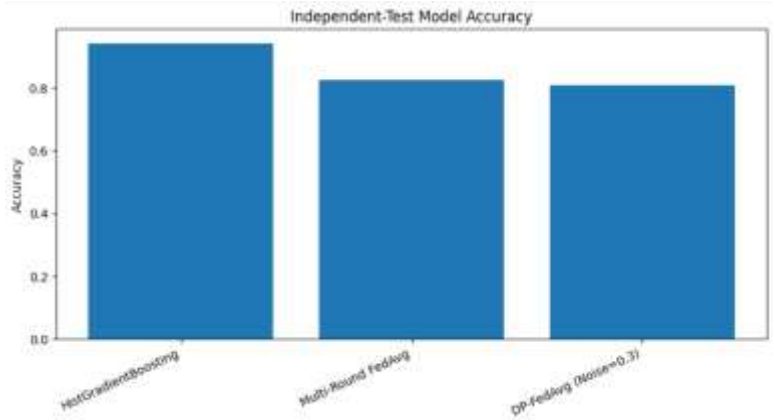


Figure 5: Independent-Test Model Accuracy Comparison

The result of the evaluation of the models is shown by the figure 6 in terms of independent-test utility metrics namely Precision, Recall and F1-score. HistGradientBoosting and Multi-Round FedAvg have values close to 0.000 while DP-FedAvg (noise = 0.3) reports Precision of around 0.0125 and Recall of around 0.0285. All the models shown have an F1 Score that is near 0.000. The model outputted by the DP-FedAvg is a utility that at least has measurable Precision and Recall under differential privacy albeit with relatively low values. These findings underline the conflicting perspectives on privacy versus predictive usefulness, pertinent to secure and trustworthy cross-border digital services in the EAC.

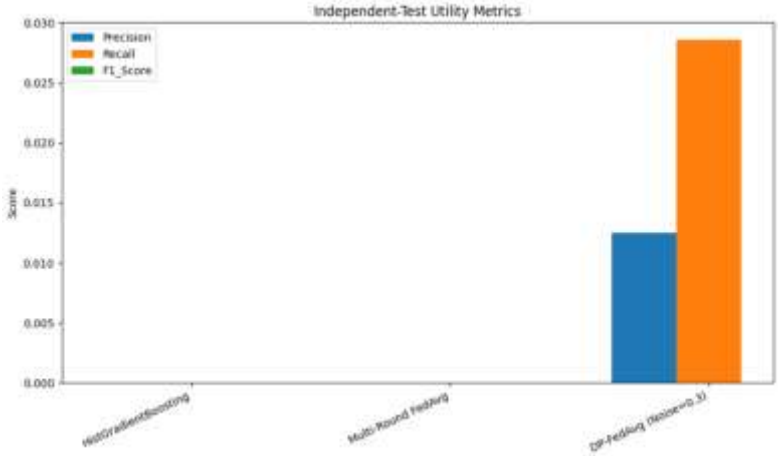


Figure 6: Independent-Test Utility Metrics Comparison

4.2 EAC Node Performance and Federated Data Distribution

American Journal of Strategic Studies
ISSN: 2790-6191 (Online)
Vol. 8, Issue No. 1, pp 83 – 104, 2026
www.carijournals.org

The figure 7 shows that independent-test accuracy of local models deployed in three EAC nodes (Kenya, Uganda and Tanzania). EAC_Kenya_Node and EAC_Uganda_Node perform the highest with an accuracy of ~1.00 (100%), suggesting that the local performance in these countries is highly consistent. The accuracy of the EAC_Tanzania_Node is around 0.82 (82%), which is 18 percentage points less than the other two nodes. The results show that it is possible to obtain high accuracy in predictions under local federated models, based on processing of data in individual national environments. At the node level, it provides support to meet the goal of the proposed architecture to promote trusted, privacy-preserving and decentralized cross-border digital services in the East African Community.

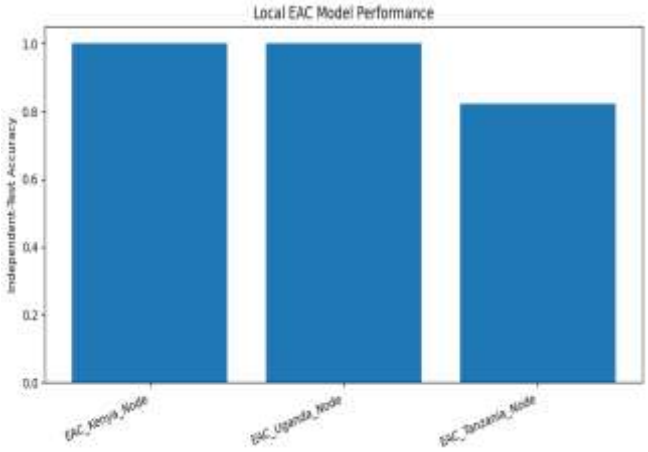


Figure 7: Local EAC Node Model Performance

The distribution of federated training data across the three EAC nodes (Kenya, Uganda and Tanzania) is shown in figure 8. The number of samples collected in each node is around 775-780, with a very even number of samples from the countries involved. Kenya sends around 775 samples, Uganda sends about 775–780 and Tanzania sends the same. The difference of the highest and lowest allocation of the data was just 5 samples, which shows that there is little imbalance in the distribution of data. A balanced participation minimises the negative impact of one country on the global federated model. The findings thus indicate the sustainability of equitable and fair training of the models, effective aggregation and privacy-preserving cross-border data exchange in the proposed East African Community digital-service architecture.

American Journal of Strategic Studies
ISSN: 2790-6191 (Online)
Vol. 8, Issue No. 1, pp 83 – 104, 2026
www.carijournals.org

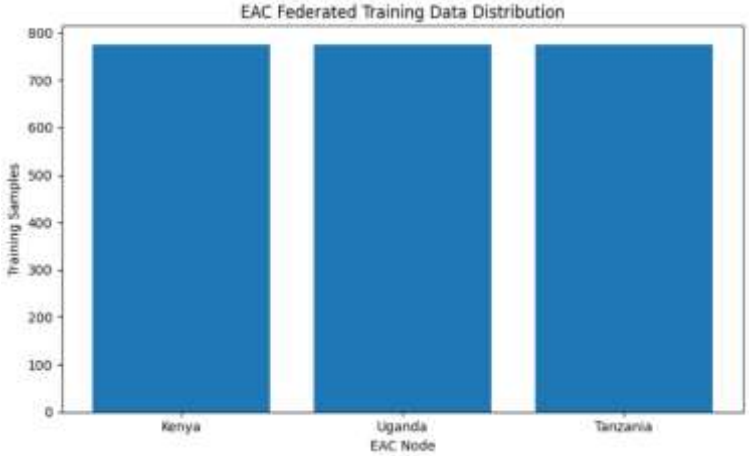


Figure 8: EAC Federated Training Data Distribution

4.3 Communication Efficiency and Scalability

Figure 9 shows that the key latency factors for cross-border communication between Kenya, Uganda and Tanzania are: The communication component is predominant for all three nodes in the EAC region, with Kenya taking around 0.45ms, Uganda and Tanzania taking around 0.5ms. There are variations in the aggregation latency, with only about 0.11ms for Kenya, 0.04ms for Uganda and 0.07ms for Tanzania. The authentication and policy-evaluation components are still relatively small, around 0.00–0.01 ms, meaning there is little overhead for processing them.

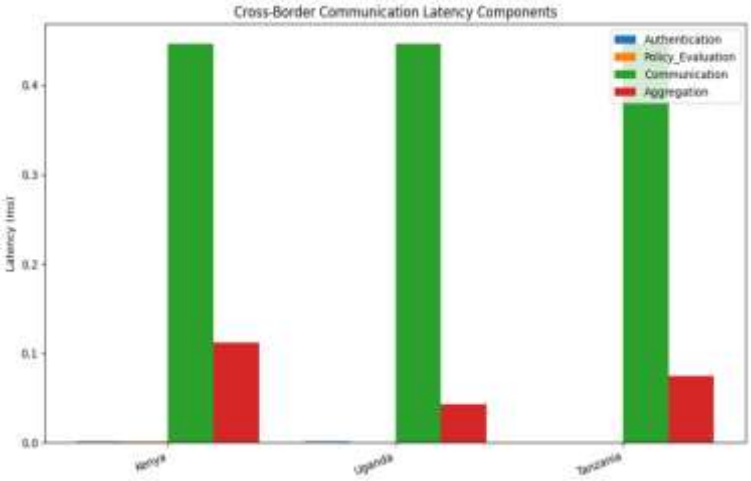


Figure 9: EAC Cross-Border Latency Comparison

Results overall show that communication represents the dominant latency contributor but authentication, policy evaluation and aggregation have relatively low levels of overhead and can enable efficient, trusted cross-border cross federation data exchange.

The cross-border communication latency for Kenya, Uganda and Tanzania in the federated data exchange architecture is shown in Figure 10. The latency recorded in Kenya is high at almost 0.61ms, in Uganda it is lowest at almost 0.50ms with Tanzania showing an intermediate latency at nearly 0.53ms. The maximum and minimum latencies varied by about

0.11ms, suggesting that the variation in participating countries was not large. These results confirm that the architecture indeed enables having low communication overhead for the cross-border digital services. This low latency enables effective federated transfer of data, timely service coordination, interoperability while maintaining privacy at the East Africa Community (EAC).

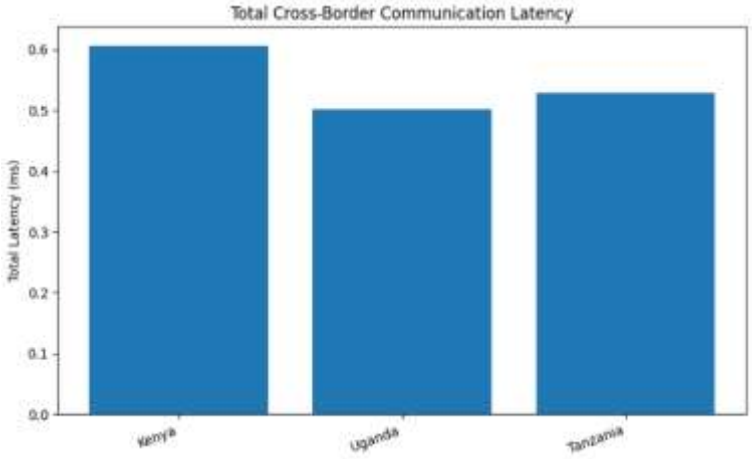


Figure 10: Federated Communication Latency across EAC

Figure 11 shows that the federated data exchange architecture becomes scalable with the number of EAC nodes from 1 to 3. The execution time with 1 node was around 390ms, 480ms with 2 nodes and 655ms with 3 nodes. This is an overall increase of about 67.9% in execution time as the nodes are increased from 1 to 3. The results show that the architecture works and delivers stability of operation as the number of participating nodes grows, while experiencing increase in computational and communication overhead as the federation size grows. This scalability highlights the architecture's potential for growth, allowing it to accommodate increasing cross-border digital services and support distributed data exchange among EAC member countries.

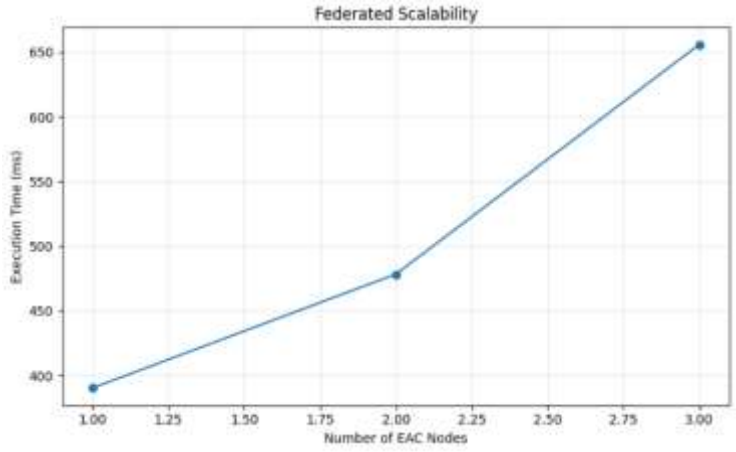


Figure 11: Federated Scalability across EAC Nodes

4.4 Security, Privacy and Classification Performance

The results of the governance and security verification for the federated data exchange architecture for preserving privacy is shown in figure 12. Each of five scenarios (legitimate Kenya node, unregistered node, unauthorized service, unauthorized role and expired access) had a Pass rating. This equates to 100% success rates for verification of the controls. Results show the capability of the architecture to be able to identify legitimate or invalid nodes, services, roles and access conditions while enforcing the trust requirements. The regular verification process ensures secure federation for all the actors in the East African Community because no one can enter without authorization or access. This constant verification helps to facilitate secure federation by all the actors of the EAC as no one can gain access or authorization. Results suggest that identity, authorization, service validation and access-expiration controls are fairly well upheld in digital services overall.

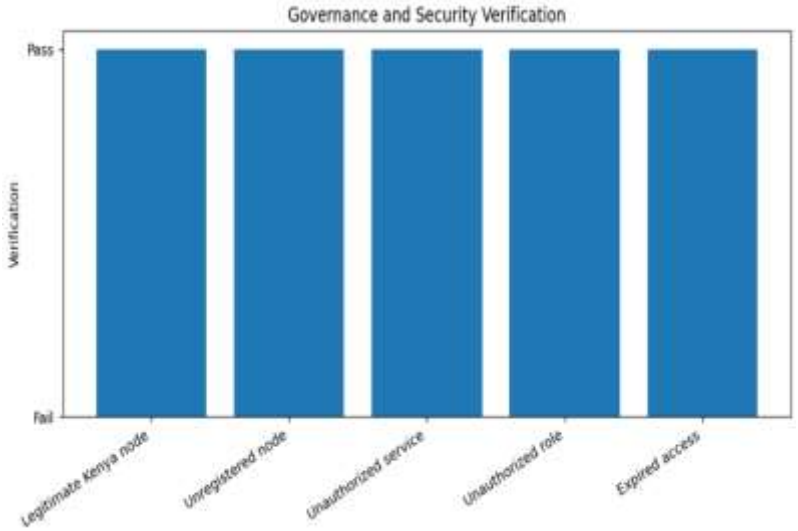


Figure 12: Governance and Security Verification Results

Figure 13 shows how the training accuracy changes with different differential privacy (DP) noise multipliers. When the noise multiplier is 0.0, the accuracy of training is around 0.658 and it is slightly reduced to 0.645 with the noise multiplier being 0.1. The best accuracy (around 0.699) was found when the noise was moderate, at 0.3. When the nail length is 0.5, however, the accuracy is significantly reduced to ~0.513 and then it falls to ~0.507 at 0.8. This is an overall decrease of approximately 22.9 percentage points from the maximum value. The results show how the increased privacy protection results in the corresponding reduction in the predictive utility of federated cross-border digital services.

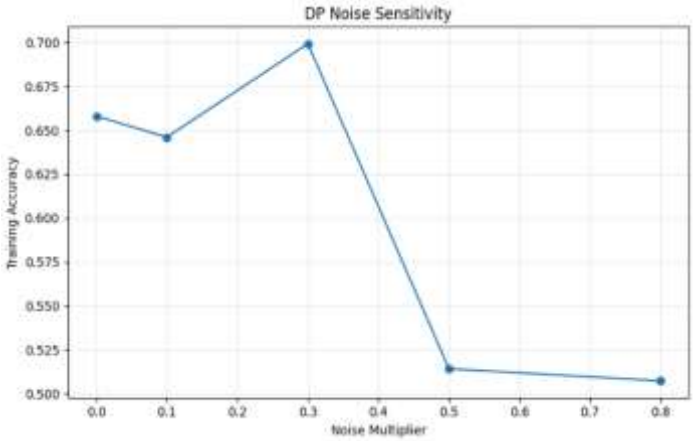


Figure 13: DP Noise Impact on Accuracy

Figure 14 shows the convergence process of the DP-FedAvg model, trained over 5 rounds of federated training. There is increasing training accuracy from Round 1 (0.50) to Round 2 (0.578) and Round 3 (0.608). There is a significant improvement in Round 4 as the accuracy reaches around 0.764 level, then a minimal loss to 0.759 in Round 5. In all, the model improves by about 25.9% in percentage points between Round 1 and Round 5, showcasing the effectiveness of converging under differential privacy. The results show that by using iterative federated aggregation, the utility of the generated model gradually increases while keeping the training process private, thus facilitating cross-border exchange of the data needed to ensure the availability of digital services.

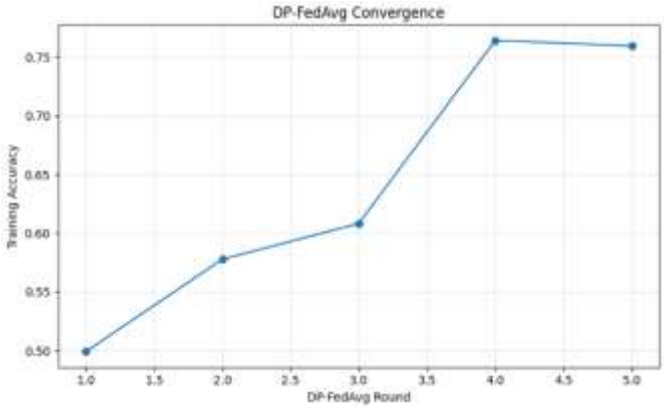
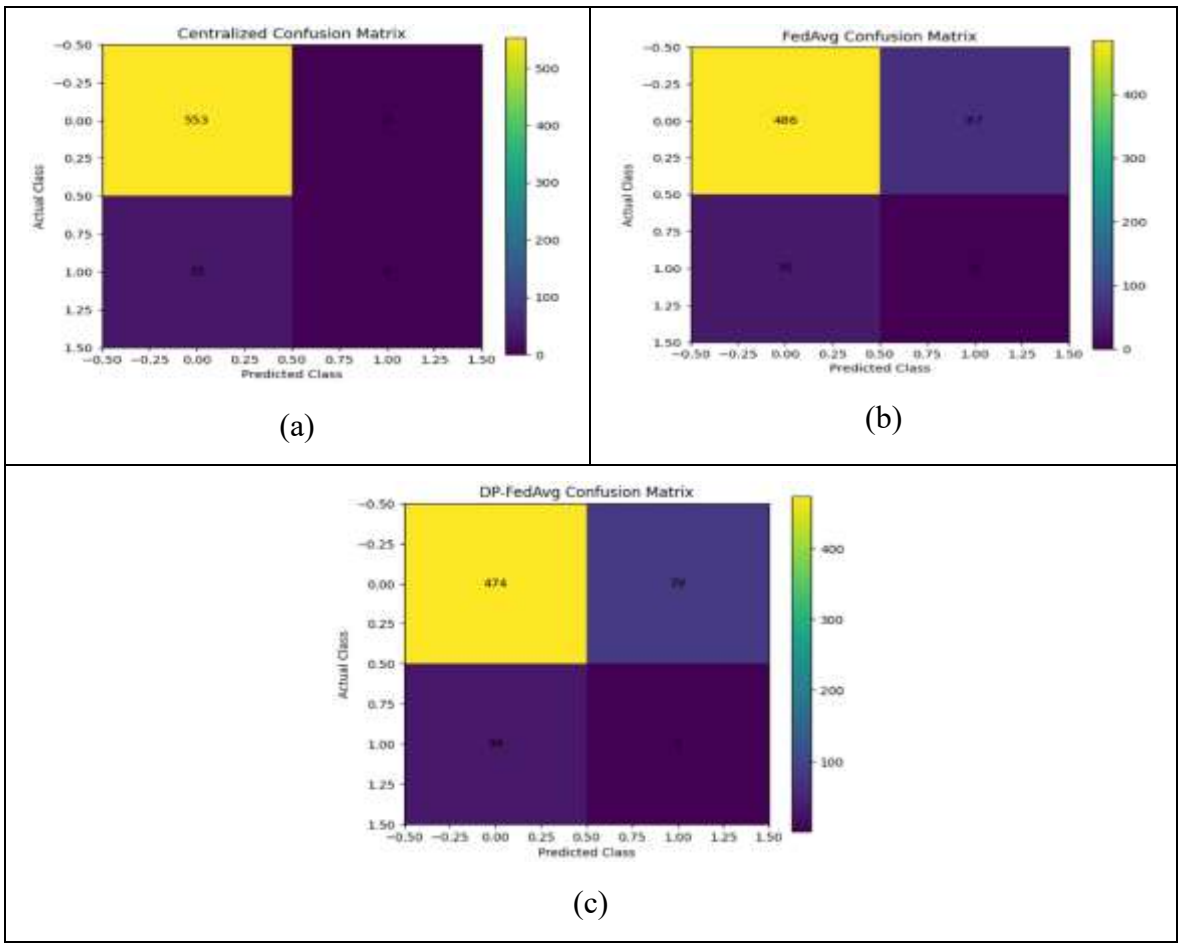


Figure 14: DP-FedAvg Convergence Performance

Confusion matrices are used for comparison of classification performance between the centralized; FedAvg and DP-FedAvg models (see Figure 15). For the centralized model with the data from Figure 15(a), 553 Class 0 samples are correctly classified and there are 35 Class 1 samples that are not. That is, the centralized model has made few minority-class predictions, but many of those that it made, it got correct.For the centralized model, using the data from Figure 15(a), 553 of the class 0 samples are correctly classified and 35 of the class 1 samples are not. That is, while the centralized model is not good at recognizing class 1, it is somewhat good at recognizing class 0. In Figure 15(a), FedAvg correctly classifies 486 Class 0 samples, while 67 are mislabeled as Class 1; moreover, 35 Class 1 samples are classified as

Class 0, meaning that FedAvg does not correctly predict any Class 1 samples. For instance, DP-FedAvg correctly classifies 474 Class 0 and 79 Class 0, 34 Class 1 sample, whereas 79 Class 0 and 34 Class 1 samples are misclassified as shown in Figure 15(c). The results prove that federated and privacy-preserving learning still achieve a substantial recognition (Class 0) while at the same time posing classification trade-offs. In general, DP-FedAvg offers privacy safeguards and efficient classification skills to trusted Cross-Border Digital Services.



(a) (b) (c)

Figure 15: Classification Performance Comparison across Centralized and Federated Learning

From the above table 1 it is clear those Huang et al. (2026) [31] has 81.2% accuracy while the proposed work has 82% accuracy. Thus, it is shown that the proposed work shows a slight improvement of 0.8 percentage points over Huang et al. (2026). This means that the federated architecture is competitive to current predictive solutions and can facilitate privacy preserving data exchange across borders. We got 82% accuracy on the independent test set with the proposed Multi-Round FedAvg model.

Table 1: Comparison of Prediction Accuracy between Existing Privacy-Preserving Federated Learning Approaches and the Proposed Work

Author & Year	Accuracy
Huang et al. (2026) [31]	81.2%
Proposed Work (2026)	**82%**

5. Conclusion

Structured approach applicable to digital services that are trusted in the East African Community, covering the concepts of institutional data sovereignty and federated learning, authentication, authorization, policy enforcement, differential privacy and auditable governance. The results of the experiments show the ability of the nodes to cooperate without providing raw data. The 775–780 samples allocated to each EAC node were very well distributed with only a 5-sample difference between the lowest and highest number of samples per node. The Multi-Round FedAvg had close to 0.82 independent-test accuracy, DP-FedAvg had 0.80 with a noise multiplier of 0.3, with a modest 0.02 drop in accuracy when protecting privacy. The five evaluated security and governance scenarios all enjoyed a 100% success rate. Communication latency was generally low, between 0.50 and 0.61ms between countries. The execution time of 390ms to 655ms shows that as the size of federation expands, there is computational overhead. The differential-privacy analysis revealed that the highest accuracy was around 0.699 at noise multiplier 0.3, before performance dropped at higher noise levels. Overall, the outcomes show that PP-FDEA can be the basis for secure, privacy-preserving and trustworthy collaboration in EAC digital services.

Reference

[1] Sifakis, Nikolaos. "Global Virtual Prosumer Framework for Secure Cross-Border Energy Transactions Using IoT, Multi-Agent Intelligence and Blockchain Smart Contracts." Information 17, no. 4 (2026): 396.

[2] Berzi, Matteo, Mattia Albertini, Ricardo Barranco, Emmanuel Brunet-Jailly, Tobias Chilla, Lewis Dijkstra, Claire Duvernet et al. "Mapping flows, shaping spaces: a review of data-driven approaches to EU cross-border regions." European Planning Studies (2026): 1-27.

[3] Li, Cong, Xinsheng Ji, Yandong Zheng and Weizhi Meng. "6G-PFIP: Privacy-Preserving and Personalized Federated Intelligent Paging for 6G Wireless Networks." IEEE Transactions on Dependable and Secure Computing (2026).

[4] Li, Dai. "AI-Driven Financial Risk Assessment and Anomaly Detection in Cross-Border Transactions: A Comprehensive Framework for Economic Security." Annals of Applied Sciences 6, no. 1 (2025).

[5] Gbenle, Peter, Olumese Anthony Abieba, Wilfred Oseremen Owobu, James Paul Onoja, Andrew Ifesinachi Daraojimba, Adebusayo Hassanat Adepoju and Ubamadu Bright

Chibunna. "A privacy-preserving AI model for autonomous detection and masking of sensitive user data in contact center analytics." World Scientific News 203 (2025): 154-193.

[6] Matta, Sai Srinivas and Manish Bolli. "Blockchain-based decentralized identity for cross-border authentication: Enhancing cybersecurity and immigration applications." ASRC Procedia: Global Perspectives in Science and Scholarship 2, no. 1 (2022): 63-88.

[7] AJUZIEOGU, UCHECHUKWU C. "Federated Learning and Privacy-Preserving Generative AI for African Contexts: A Research Framework."

[8] Anin, Johnson, Muhammad Jahanzeb Khan, Omar Abdelsalam, Mahmoud Nabil, Fei Hu and Ahmad Alsharif. "Efficient and privacy-preserving ConvLSTM-based detection of electricity theft cyber-attacks in smart grids." IEEE Access 12 (2024): 153089-153104.

[9] van Reisen, Mirjam, Samson Yohannes Amare, Ruduan Plug, Getu Tadele, Tesfit Gebremeskel, Abdullahi Abubakar Kawu, Kai Smits et al. "Curation of federated patient data: a proposed landscape for the African Health Data Space." In Federated learning for digital healthcare systems, pp. 59-80. Academic Press, 2024.

[10] Acheampong[1], Eric and Tobias Kwame Adukpo. "Data-Driven risk assessment framework for federal grant accountability in US state-administered social service and community development programs."

[11] Song, Lingqiao. Cross-border human genomic data sharing in the United States and China: Can a cosmopolitan perspective on genomics provide a way forward?. McGill University (Canada), 2025.

[12] Beduschi, Ana. "Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations." Data & Policy 3 (2021): e15.

[13] Michael, Meyo Otieno. "Privacy preserving data governance in cross border Telemedicine using federated learning and differential Privacy in Kenya." PhD diss., Cuk, 2025.

[14] Rallabandi, Bhaskara Raju, Karthick Cherladine, Siva Sudheer Mahadasu and Neelakantam Gudla. "Intent-Driven MVNO Architecture for Cross-Border 5G/6G Networks in Africa: Toward the One Africa Digital Economy." In 2025 IEEE Connecting the Unconnected Europe, Middle East and Africa Regional Summit (CTUS-EMEA), pp. 1-11. IEEE, 2025.

[15] Nwokedi, Nwannebuike and Olakunle Saheed Soyege. "Advances in AI and Machine Learning for Antimicrobial Resistance Monitoring and Healthcare Diagnostics." world Scientific News 203 (2025): 79-109.

[16] Mpofu, Patience, Solomon Hopewell Kembo, Marlvern Chimbwanda, Saulo Jacques, Nevil Chitiyo and Kudakwashe Zvarevashe. "A privacy-preserving federated learning architecture implementing data ownership and portability on edge end-points." International Journal of Industrial Engineering and Operations Management 5, no. 2 (2023): 118-134.

[17] Zhang, Fan, Daniel Kreuter, Javier Fernandez-Marques, Gregory Verghese, Bernard Butler, Nicholas Lane, Suthesh Sivapalaratnam et al. "Building Privacy-and-Security-

Focused Federated Learning Infrastructure for Global Multi-Centre Healthcare Research." arXiv preprint arXiv:2603.10063 (2026).

[18] Meyo, Michael, Cynthia Ikamari and Anthony Mile. "A Privacy-Preserving Data Governance in Cross-Border Telemedicine Using Federated Learning and Differential Privacy in Kenya." (2025).

[19] Ibor, Ayei, Mark Hooper, Carsten Maple, Jon Crowcroft and Gregory Epiphaniou. "Considerations for trustworthy cross-border interoperability of digital identity systems in developing countries." AI & society 40, no. 4 (2025): 2729-2750.

[20] Lin, Jiling. "Design and Simulation of a Federated Learning-Based Multilateral Data Privacy Protection and Ethical Collaborative Governance Model for Cross-Border E-Commerce." In Proceedings of the 2025 5th International Conference on Internet of Things and Machine Learning, pp. 324-330. 2025.

[21] Sarhan, Akram Y. "An agent-based secure privacy-preserving decentralized protocol for sharing and managing digital health passport information during crises." PeerJ Computer Science 9 (2023): e1458.

[22] Joseph, Mtakai N. "Cross-Border Cyber Threat Intelligence Sharing Between East African Community (EAC) Member States: Legal, Technical and Trust Barriers for Regional SOC Collaboration (Focus on Kenya–Uganda–Tanzania)."

[23] Okwor, Zikora. "Harmonising AI Regulation under the AfCFTA: Challenges and Opportunities for Cross-Border Governance." Covenant University Journal of Politics and International Affairs (2026): 28-28.

[24] Ebabu, Engidaw Abriham, Haichun Yu, Zou Weikang, Huang Yixiong and Ayele Addis Ambelu. "Navigating sustainable digital transformation in South-South cross-border E-Commerce: Insights on cultural adaptation, green marketing strategy and inclusive business model innovation." International Review of Economics & Finance (2026): 104907.

[25] Sampson, Emmanuel and Abena Serwaa Annor. "Cross-Border E-Commerce in Africa: Can Digital Sales Infrastructure Bridge Global Trade Gaps." (2025).

[26] Mutesi, Josephine, Samuel Mutarindwa, Alice Mukasekuru and Gilbert Shyaka. "Digital readiness and business performance of Rwandan women entrepreneurs in cross-border trade under the African Continental Free Trade Area (AfCFTA)." Cogent Business & Management 12, no. 1 (2025): 2518248.

[27] Olalekan, Olatunbosun Onaopemipo, Deborah Oluwadamilola Adeleye and Vivek Kumar Srivastava. "The surge of cross-border payment firms in Africa: Implications for entrepreneurship and SMES." International Journal of Science and Research Archive 13, no. 1 (2024): 684-696.

[28] Panga, Faustine, Richard Manase Nkunda and Apio Scovia. "Customs clearance procedures and Cross-border Logistics performance in East Africa: a case of Malaba-Busia and Taveta-Holili one-stop Border Posts." Journal of Co-operative and Business Studies (JCBS) 8, no. 1 (2024).

[29] Ahmed, Bilal. "Cross-Border Connectivity: Strengthening Economic Ties and Regional Integration." Journal of Regional Connectivity and Development 3, no. 1 (2024): 70-84.

[30] Subramanian, C. Bala. "Iot Enabled Privacy Preserving In Federated Hybrid Smart Grid Cloud Environment Using Spark." (2020).

[31] Abraham, Igbajar and K. C. Nwachukwu-Nwokeafor. "A FEDERATED FRAMEWORK FOR PRIVACY-PRESERVING HEALTH DATA SHARING ACROSS AFRICAN BORDERS."

[32] Huang, Kui, Yinzhen Wei, Tengqiao Kong, Hongyu Chen, Zongshan Wang, Dongmei Zhang and Guancheng Chen. "A federated learning-based privacy-preserving prediction model for cross-organizational data governance." Journal of King Saud University Computer and Information Sciences (2026).

[33] https://www.kaggle.com/datasets/nxpnsv/country-health-indicators

[34] Alaridhi, Esraa Mohammed Ali Jaber and Duaa Shaker Naji. "Blockchain-Based Digital Identity Management: A Comprehensive Review of Security, Privacy, Regulatory Perspectives and Future Directions." *Journal of Kerbala University* 22, no. 4 (2025): 142-160.

[35] Amebleh, J. and D. A. Onoja. "Privacy-preserving consumer-behavior analytics across multistate telemedicine: Differential privacy, k-anonymity, & federated gradient aggregation." *Acta Scientifica Malaysia(ASM)* (2025).

[36] Berzi, Matteo, Mattia Albertini, Ricardo Barranco, Emmanuel Brunet-Jailly, Tobias Chilla, Lewis Dijkstra, Claire Duvernet et al. "Mapping flows, shaping spaces: a review of data-driven approaches to EU cross-border regions." *European Planning Studies* (2026): 1-27.

[37] Rehan, Hassan. "Bridging the digital divide: A socio-technical framework for AI-enabled rural healthcare access in developing economies." *Euro Vantage journals of Artificial intelligence* 2, no. 1 (2025): 19-27.

[38] Sarhan, Akram Y. "An agent-based secure privacy-preserving decentralized protocol for sharing and managing digital health passport information during crises." *PeerJ Computer Science* 9 (2023): e1458.

[39] Tam, Prohim, Riccardo Corrado and Trang Thi Pham. "Exploring responsible innovation with privacy preservation: federated learning policies for digital finance services in Asia." Special theme: Digitalization as an opportunity for inclusive growth in Asia and the Pacific 215 (2025).

[40] Dlamini, Thando, Lerato Maseko, Sipho Nkosi, Zinhle Khumalo, Jabulani Ndlovu, Austin Smith and Andile Tshabalala. "Evaluation of Collaborative Data Sharing Mechanisms for Comprehensive Cyber Threat Mitigation in National Security Crises." *Int. J. Appl. Soc. Anal* 9 (2024): 1-22.