International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V74I7P102

Volume 74 Issue 7, 7-22, July 2026

Original Article

Federated Sovereign AI Ecosystems: A Framework for Trusted Governance and Cross-Border Intelligence Interoperability

Abdinasir Ismael Hashi[1], Abdirizak Mohamed Hashi[2], Osman Abdullahi Jama[3]

[1,3]*Computer Science, Somali National University, Mogadishu, Somalia.*
[2]*Computer Science, Jazeera University, Mogadishu, Somalia.*

[1]*Corresponding Author : nasirhaji@snu.edu.so*

Received: 25 May 2026 Revised: 29 June 2026 Accepted: 14 July 2026 Published: 30 July 2026

Abstract - *The use of Artificial Intelligence (AI) in Cybersecurity and cross-border intelligence sharing has increased in relevance and importance in recent years; however, current Centralised AI architectures are plagued with data privacy, Digital sovereignty, Governance and regulatory compliance concerns. This study introduces a Federated Sovereign AI Ecosystem (FSAIE) designed to foster the sharing of intelligence within a federated learning framework, securely integrate data interoperability, and ensure national data sovereignty and trusted Governance. Testing of the framework was conducted on the UNSW-NB15 cybersecurity dataset that consists of 257,673 network traffic records with 49 features, and the World Governance Indicators (WGI) dataset. Four models (Random Forest, XGBoost, Deep Neural Network (DNN), Federated Learning) were built and evaluated for accuracy, precision, recall, F1-score, ROC-AUC, trust index, interoperability and communication cost. The experimental results show that the XGBoost model has the highest "accuracy (99.05%), precision (99.50%), recall (99.01%), F1 score (99.25%) and ROC-AUC (0.9995%)" than the Random Forest model (accuracy: 98.08%) and DNN model (accuracy: 97.18%). The proposed ecosystem also showed an impressive Trust Index of 94.56 and achieved a 100% efficiency in intelligence exchange and a communication cost of 21,096.22 KB per round, which establishes a secure and efficient cross-border collaboration. The proposed FSAIE is a scalable, privacy-first, and governance-enlightened solution closely balancing predictive performance with trusted interoperability and national data sovereignty to make collaborative AI-driven cybersecurity applications a reality.*

Keywords - *Federated Sovereign AI; Federated Learning; Trusted Governance; Cross-Border Intelligence Interoperability; Data Sovereignty; Cybersecurity.*

1. Introduction

It can perform tasks such as intelligent decision making, data analysis, and automation, which have already been instrumental in the field of Artificial Intelligence (AI) that is transforming business, government, and society [1]. It is clear that nations throughout the globe will rely on AI-based applications in essential fields and regions like Cybersecurity, defense, national security, intelligence analysis, public administration and public security and must ensure that they will be able to work with other nations with a sense of reliability. [2] The architectures of the traditional AI systems are based on centralized data collection and processing techniques, which involve gathering sensitive information and its subsequent analysis within a single information system.

While the methods may give, e.g., very high prediction accuracy, there are many issues concerning privacy, security, sovereignty, regulations and trust [3]. The issues are more complex in the international arena, though, as countries have to collaborate on matters while safeguarding their own information and assets.

One of these concepts that has swept the past few years was Digital sovereignty, which has been a primary concern of the governments regarding the protection of their national interests and confidential information regarding third-party access or impact [4]. Data sharing without restrictions between different countries is becoming more challenging as countries have begun enacting regulations on related issues such as data localization, privacy protection, Cybersecurity etc.

According to the recent trends, cyber-crimes, transnational crime, terrorism and geopolitical threats are increasing, hence there is a need for intelligence sharing mechanisms across borders [5]. So, there is a need to develop frameworks that allow safe intelligence cooperation, maintaining the sovereignty of nations and adhering to various legislations and regulations [6]. To address this challenge, new federated and decentralized AI architectures have been explored that enable collaborative learning without exposing sensitive data. To meet this challenge, new federated and decentralized AI systems have been explored, which enable collaborative learning without exposing sensitive data.

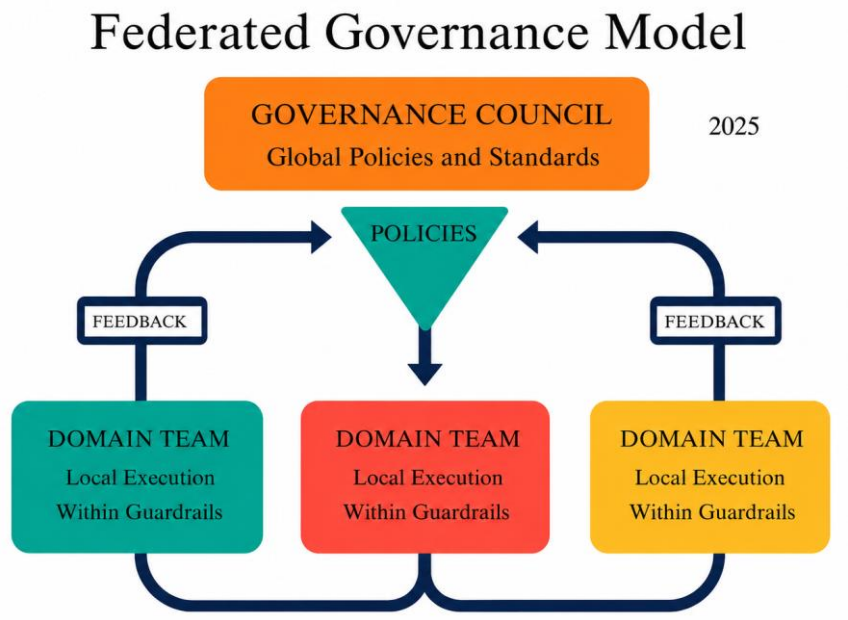


Fig. 1 Federated governance model

One approach to tackle these concerns has been identified as Federated Learning (FL). Federated learning differs from the traditional 'centralized' machine learning model by enabling multiple organizations or independent units to collectively train an AI-based model without the need for data sharing between the facilities [7]. Low risk of privacy concerns and regulatory compliance due to the sharing of only model parameters and learnt knowledge among participants [8]. The decentralized learning model resembles the notions of sovereign Governance in which countries are autonomous and have control over their own information assets, but contribute to the formation of collective intelligence [9]. However, to achieve the benefits of federated AI ecosystems, the technical components are not enough; there is a need for trusted governance arrangements, interoperability protocols, security protocols, and accountability frameworks to ensure that the various parties can work together responsibly with one another [10].

Another key need for today's AI ecosystems is cross-border intelligence interoperability. In the past, intelligence information was collected from various sources, such as critical infrastructure networks, surveillance networks, government databases, and cybersecurity systems [11]. They are often under distinct Governance, standards and formats, which can hinder effective information flow. Communication and coordination with other intelligence operations may be compromised by interoperability problems, which can reduce their effectiveness in responding to a new or evolving threat [12]. Thus, it is necessary to create a framework that allows for the easy transfer, semantic coherence, secure transfer of information and mutual trust between sovereign participants for meaningful international cooperation.

Trusted Governance is an indispensable component to building these interoperable ecosystems. Governance should ensure transparency, accountability, fairness, legality, and ethical use of AI [13]. Also, it would establish processes for assessing trustworthiness, authentication, authorization, policy enforcement and managing risks, thus preserving the confidence between intercommunicating sovereign agents. The union of these governing principles and the enabling technologies of federated learning and secure interoperability will ensure an environment in which intelligence sharing is managed, transparent, and lawful [14].

The present research focuses on designing a Federated Sovereign AI Ecosystem that will facilitate Governance and interoperability of cross border intelligence. In the proposed framework, federated learning, trust measurement based on governance indicators, security and privacy preservation techniques, cybersecurity intelligence, and interoperability strategies have been integrated to foster collaboration and sharing of information among sovereign entities. With the inclusion of governance factors into intelligent systems, an attempt has been made to develop a robust and scalable ecosystem that would help in enhancing collective decision-making processes. The goal of the research is thus to build a connection between innovations and Governance needs in the domain of artificial intelligence. Objectives of the research are:

2. Related Work

The increasing importance of data sovereignty, compliance, and cross-border collaboration within the context of technological innovation and the development of federated infrastructures and architectures is emphasized in the latest literature on Sovereign AI, federated infrastructures, and cross-border intelligence interoperability. Motgi et al. (2026) [15] presented a federated infrastructure blueprint for Sovereign AI that includes jurisdiction-aware workload placement, federated data management, and compliance monitoring features for safe and secure deployment of AI across multi-cloud

environments. Like Odion et al. (2026) [16] proposed, the Integrated AI Risk Governance Framework (IARGF) encompasses policy and institutional, technical, and operational governance aspects while explicitly recognizing digital sovereignty as a governance aim. Singh et al. [17] defined sovereign AI as a spectrum, with autonomy and cooperativeness being the two extremes of the continuum, highlighting the need to strike a balance between the two. In addition, Agarwal et al. (2026) [18] provided an holistic AI governance framework for India, which highlights the importance of federated standards for cross-sector and cross-border AI governance without centralizing Governance. The studies highlight the need for interoperability of Governance, regulatory, and digital infrastructure, along with adaptive frameworks, to build trust, accountability, and compliance in cross-jurisdictional contexts, to achieve effective Sovereign AI ecosystems.

As for technologies, Federated Learning and Privacy-Preserving Machine Learning are seen as the key technologies for secure cross-border intelligence sharing. Gajula et al. (2025) [19] showed the federated learning approach to enable collaborative financial risk analysis, keeping the data sovereignty intact by sharing encrypted models. Foster et al. (2026) [20] compared these approaches to ensure privacy while maintaining utility, such as federated learning, differential privacy, homomorphic encryption and secure multi-party computation, and determined that federated learning combined with differential privacy provided a “sweet spot” for privacy whilst also being useful. Lopez et al. (2024) [21] presented a framework named Adaptive Collaborative Intelligence (ACI), which integrates federated learning, reinforcement learning and Bayesian inference to enhance the international cyber-threat detection and response capability.

Likewise, Lin and others (2025) [22] proposed a new federated system using blockchain, differential privacy, and automated Governance to increase the security of privacy, coordination, and inter-jurisdictional protection of privacy. Subramanian et al. (2024) [23] also emphasized the importance of federated AI for achieving regulatory compliance in various legal frameworks and for collaborative model development. Overall, these studies underscore the pivotal role of federated and privacy-preserving AI technologies as key enablers in the Governance and interoperability of AI intelligence, enabling trusted cross-border AI ecosystems.

3. Research Methodology

This research used a quantitative and simulation approach to design a Federated Sovereign AI Ecosystem for cross-border and trustworthy sharing of intelligence and information, while ensuring national data sovereignty.

This study utilized cybersecurity intelligence information using the UNSW-NB15 dataset and governance factors using the World Governance Indicators dataset. It combines FL, Trusted Governance, and secure interoperation technology to test the performance of sharing intelligence information between sovereign entities.

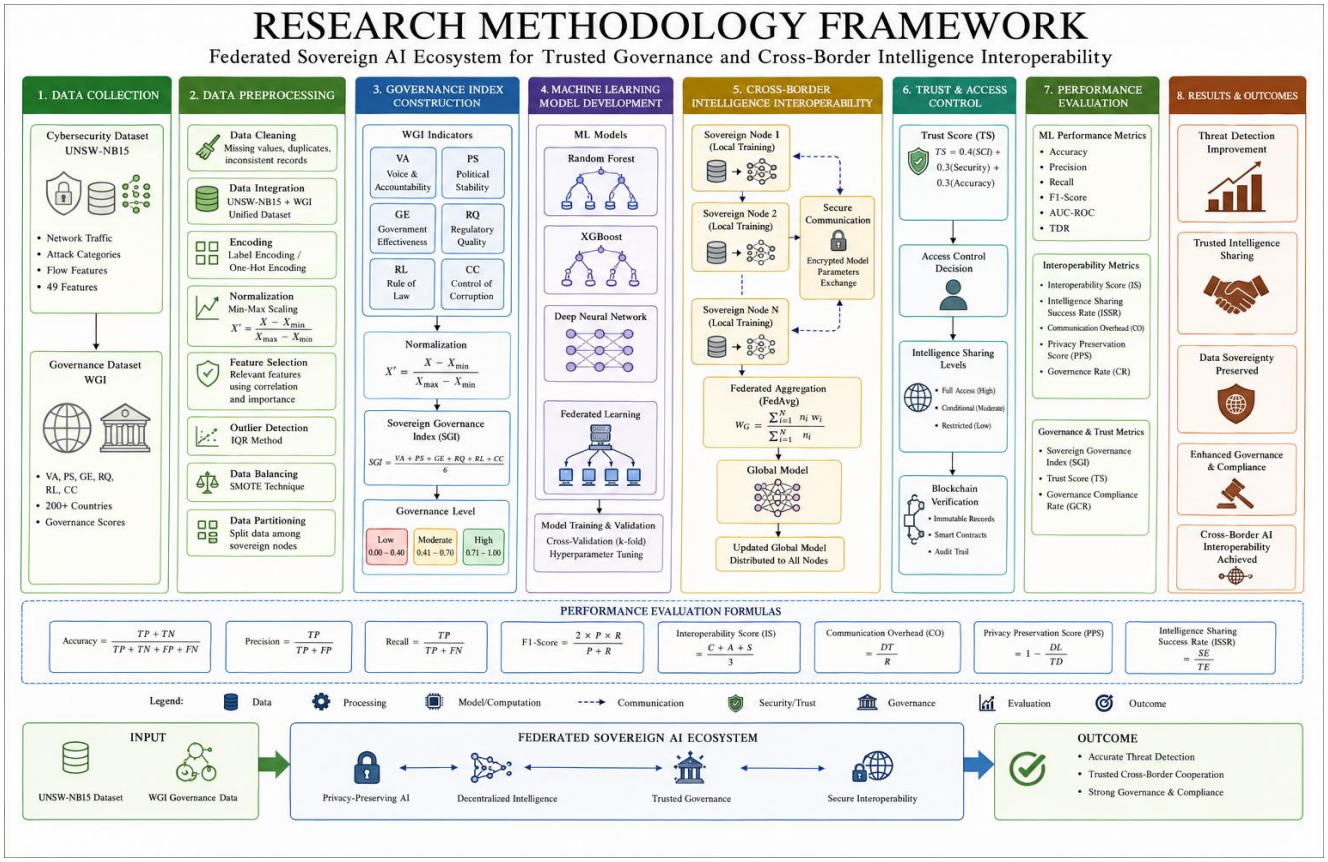


Fig. 2 Research methodology framework

3.1. Dataset Collection

Data collection is a crucial phase of the proposed Federated Sovereign AI Ecosystem development. Secondary datasets extracted from the open and globally acclaimed sources were utilized in order to achieve a reliable, reproducible, and scalable nature of the research framework. Two different datasets were exploited:-UNSW-NB15 dataset for cyber security intelligence and-World Governance Indicators (WGI) dataset.

3.1.1. Collection of Cybersecurity Intelligence Data

The cybersecurity module of the study is designed based on the UNSW-NB15 dataset [24]. This data was created at the Cyber Range Laboratory of the Australian Centre for Cyber Security and consists of the records of contemporary network traffic with both malicious and non-malicious behavior. The UNSW-NB15 dataset contains nearly 257,673 network traffic samples with 49 network features and attack labels. The different types of attacks are categorized into Fuzzers, Backdoors, Analysis, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.

3.1.2. Collection of Governance and Sovereignty Data

The World Bank World Governance Indicators (WGI) dataset [25] is used for assessing the trusted Governance and national sovereignty dimension. The Governance Data includes indicators of institutional effectiveness, regulatory quality, political stability, accountability and rule of law, as well as a measure of Governance for each country in the world. They are key measures to evaluate the capacity of sovereign bodies to join and be part of collaborative AI ecosystems.

This dataset contains governance indicators for over 200 countries: “Government Effectiveness (GE), Regulatory Quality (RQ), Rule of law (RL), Control of Corruption (CC), Political Stability (PS) and Voice and Accountability (VA)”. The data associated with countries that participate in the process is extracted and then transformed into governance scores, which refer to the trustworthiness and maturity of Governance within each sovereign node of the federated ecosystem.

Table 1. 49 Features of the dataset

No.	Feature	No.	Feature	No.	Feature	No.	Feature	No.	Feature
1	srcip	11	dttl	21	stcpb	31	sintpkt	41	ct_srv_src
2	sport	12	sloss	22	dtcpb	32	dintpkt	42	ct_srv_dst
3	dstip	13	dloss	23	smeansz	33	tcprtt	43	ct_dst_ltm
4	dsport	14	service	24	dmeansz	34	synack	44	ct_src_ltm
5	proto	15	sload	25	trans_depth	35	ackdat	45	ct_src_dport_ltm
6	state	16	dload	26	res_bdy_len	36	is_sm_ips_ports	46	ct_dst_sport_ltm
7	dur	17	spkts	27	sjit	37	ct_state_ttl	47	ct_dst_src_ltm
8	sbytes	18	dpkts	28	djit	38	ct_flw_http_mthd	48	attack_cat
9	dbytes	19	swin	29	stime	39	is_ftp_login	49	label
10	sttl	20	dwin	30	ltime	40	ct_ftp_cmd		

3.2. Data Preprocessing

Data preprocessing is a crucial stage in the proposed Federated Sovereign AI Ecosystem because the collected data originate from heterogeneous sources, namely the UNSW-NB15 cybersecurity dataset and the WGI dataset.

3.2.1. Data Cleaning

The first step is to recognize and eliminate incomplete, duplicate, and contradictory records from both sets of records. There could be missing values due to faulty network traffic data or lacking governance scores. Mean imputation is performed on numerical missing values, and mode imputation is used for categorical missing values. Mean imputation for a feature X is denoted as:

$$X_{missing} = \frac{\sum_{i=1}^{n} X_i}{n}$$

where:

- X_i signifies available observations.
- n represents the number of valid records.

The duplicate entries are deleted to prevent bias in model training. The data set excludes records of invalid network traffic with corrupted values.

3.2.1. Data Integration

Cybersecurity intelligence information extracted from UNSW-NB15 and Governance information extracted from WGI are brought under a single analysis frame. The sovereign nodes are assigned the scores that match their countries’ Governance while retaining their cybersecurity information.

The dataset is thus formulated as:

$$D_{Integrated} = D_{Cybersecurity} \cup D_{Governance}$$

where:

- $D_{Cybersecurity}$ represents network intelligence records.
- $D_{Governance}$ represents governance indicators.

This will ensure analysis of both security information and governance readiness together.

3.2.2. Categorical Data Encoding

The UNSW-NB15 data set contains features such as type of protocol, type of service, class of attack and so on, which are categorical. These variables are converted to numerical value using Label encoding and One-Hot Encoding.

To improve machine learning model accuracy and remove ordinal biases, one-hot encoding transforms category information into binary vectors.

3.2.3. Data Normalization

As the features extracted are of different scales and units, a normalization technique is applied to make the features uniform. Features like Packet size, Flow duration, trust score and indicators of Governance were normalized between 0 and 1 range using Min-Max normalization.

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where:

- $X$is the original value.
- $X_{min}$is the minimum value.
- $X_{max}$is the maximum value.
- $X'$is the normalized value.

Normalization avoids large-scale variables from dominating the learning process.

3.2.4. Feature Engineering

Feature engineering is done to construct additional features that improves the prediction performance of the federated learning model.

Sovereign Governance Index (SGI)

A composite governance score is created using key WGI indicators:

$$SGI = \frac{GE + RQ + RL + CC}{4}$$

where:

- GE = Government Effectiveness
- RQ = Regulatory Quality
- RL = Rule of Law
- CC = Control of Corruption

The SGI reflects the governance maturity of each sovereign participant.

Trust Score (TS)

The trustworthiness of a participating node is computed as:

$$TS = 0.4(SGI) + 0.3(Security) + 0.3(Accuracy)$$

where:

- SGI = Sovereign Governance Index
- Security = Cybersecurity Score
- Accuracy = Local Model Accuracy

The Trust Score is later used for access control and intelligence-sharing decisions.

Table. 2 Trust score level

Score	Trust Level
0–40	Low
41–70	Medium
71–100	High

3.2.5. Federated Data Partitioning

To mimic the cross-border intelligence interoperability, the processed dataset is partitioned into different sovereign nodes, where each node would have its local data and train its own machine learning model.

If the complete dataset is signified by D, then:

$$D = \{D_1, D_2, D_3, \dots, D_n\}$$

where:

- D_i signifies the local dataset of sovereign node i.
- n characterizes the total number of participating countries.

Data sovereignty is also maintained, as raw data does not leave local jurisdiction.

3.3. Cross-Border Intelligence Interoperability

One of the essential features of the proposed Federated Sovereign AI Ecosystem is Cross-Border Intelligence Interoperability, which allows multiple sovereign nations and intelligence agencies to share intelligence insights securely while maintaining data sovereignty, privacy, and regulatory compliance. Sensitive data exchange across organizational and national boundaries within the traditional intelligence sharing mechanisms is often done through centralized architectures, posing serious questions of security, confidentiality, and legal compliance. The proposed framework tackles these challenges through federated learning, trusted governance structures and secure communication channels to enable collaborative intelligence generation without the sharing of raw data. Each sovereign entity maintains control of its local data sets and shares secure parameters with other sovereign entities in order to participate in the model of the intelligence. This will not only keep national security information under its control, but also allow it to take advantage of international intelligence sharing.

The interoperability framework combines cybersecurity data from the UNSW-NB15 dataset with governance data from the Worldwide Governance Indicators (WGI) dataset. The sovereign participants are modeled as autonomous nodes that train local machine learning models with their own intelligence data. Different nodes' governance capabilities are assessed by the Sovereign Governance Index (SGI), which reflects the institutional effectiveness, regulatory quality, rule of law, political stability, accountability and corruption control. These governance evaluations are used as part of the trust management system to decide the eligibility and degree of participation of the individual entities in the intelligence sharing ecosystem. As a result, those countries with more robust Governance and trust scores receive more freedom of access to intelligence collaboration activities.

3.4. Machine Learning Model Development

The focus of the ML Model Development stage is to construct the intelligent models that will perform the task of detecting cyber threats, evaluating trust and ensuring safe

sharing of intelligence for decision-making within the envisioned Federated Sovereign AI Ecosystem. The dataset UNSW-NB15 is employed for cybersecurity threat detection, whereas governance indicators of WGI are used to assess trust and Governance. Different ML models are built, and their effectiveness in cyber-security threat detection for cross-border intelligence interoperability is compared; the selected models are Random Forest, XGBoost, DNN and FL. These ML models are trained on the preprocessed cybersecurity features, and their performance is tested using common metrics: “Accuracy, Precision, Recall and F1-Score”.

3.4.1. Random Forest (RF)

Random Forest refers to ensemble learning algorithms that utilize various decision trees in order to enhance classification accuracy and avoid overfitting [26].

This algorithm works well in solving cybersecurity problems due to its ability to work with high-dimensional data and detect complicated patterns of attacks. When training a Random Forest, many decision trees are constructed using random sub-samples of data and attributes.

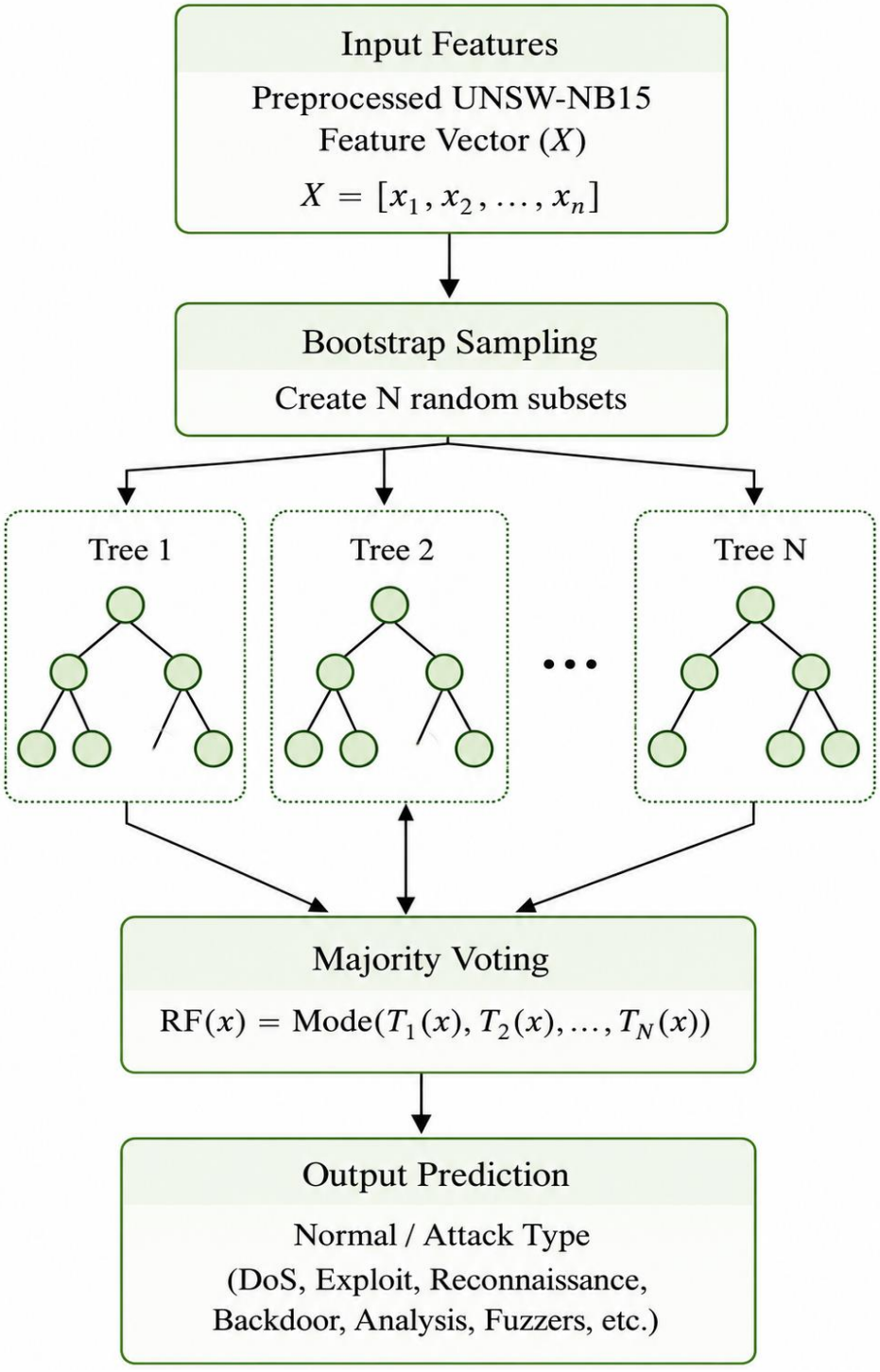


Fig. 3 RF architecture

Final output prediction is achieved based on a voting system between all the trees. The function for classification in the Random Forest model can be described as:

$$RF(x) = Mode(T_1(x), T_2(x), \ldots, T_n(x))$$

where:

- $T_1, T_2, \ldots, T_n$ represent decision trees.
- x denotes the input feature vector.
- Mode represents the majority voting mechanism.

This study utilizes the Random Forest method to categorize network traffic as either normal or malicious. The Random Forest algorithm is trained on traffic patterns linked to cyber-attacks, including DoS, Exploits, Reconnaissance, and Backdoors found in the UNSW-NB15 dataset.

3.4.2. Extreme Gradient Boosting (XGBoost)

XGBoost is a sophisticated boosting technique that combines trees iteratively, reducing the classification errors of the previous tree. This is in contrast to Random Forest, where each tree is built independently. The resulting tree models are combined together, each focusing on the residual errors of previous tree models [27], producing high classification performance for sophisticated cyber data.

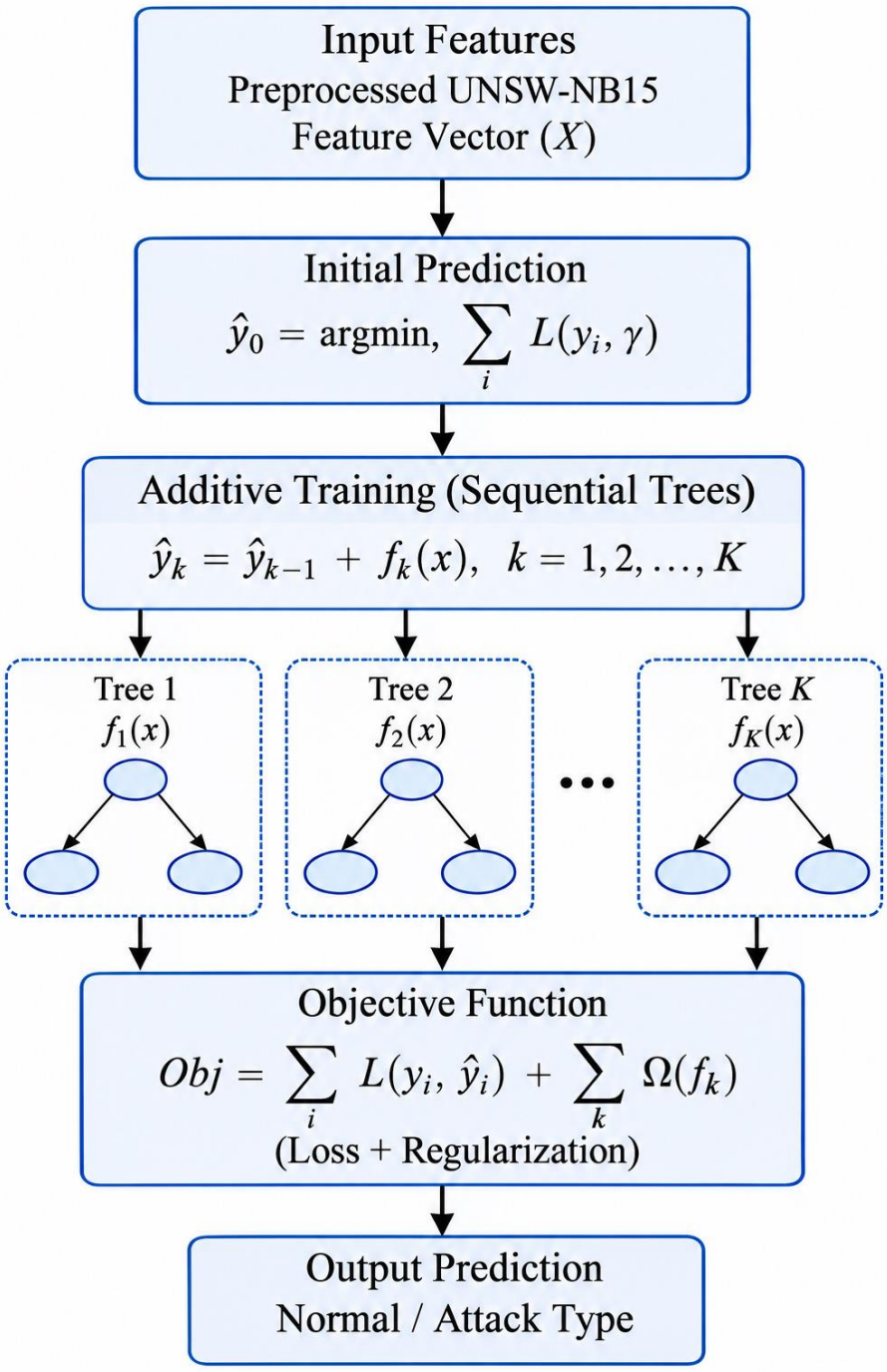


Fig. 4 XG-Boost architecture

The prediction function of XGBoost is:

$$\hat{y} = \sum_{k=1}^{K} f_k(x)$$

where:

- $\hat{y}$ is the predicted output.
- $f_k(x)$ signifies the k^{th}decision tree.
- K represents the total number of trees.

The objective function is defined as:

$$Obj = \sum_{i=1}^{n} L(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k)$$

where:

- L is the loss function.
- Ω is the regularization term.

In the proposed system, XGBoost can be used for more accurately detecting threats and subtle attack behaviors. Since XGBoost can capture the nonlinear relationship between the variables and can also handle class imbalance, it would yield good results.

3.4.3. Deep Neural Network (DNN)

Deep Neural Networks are machine learning algorithms that have the capability to extract hierarchical representations of features from huge amounts of data [28]. DNN is made up of an input layer, hidden layers, and an output layer. Each neuron receives inputs using weights and activation functions.

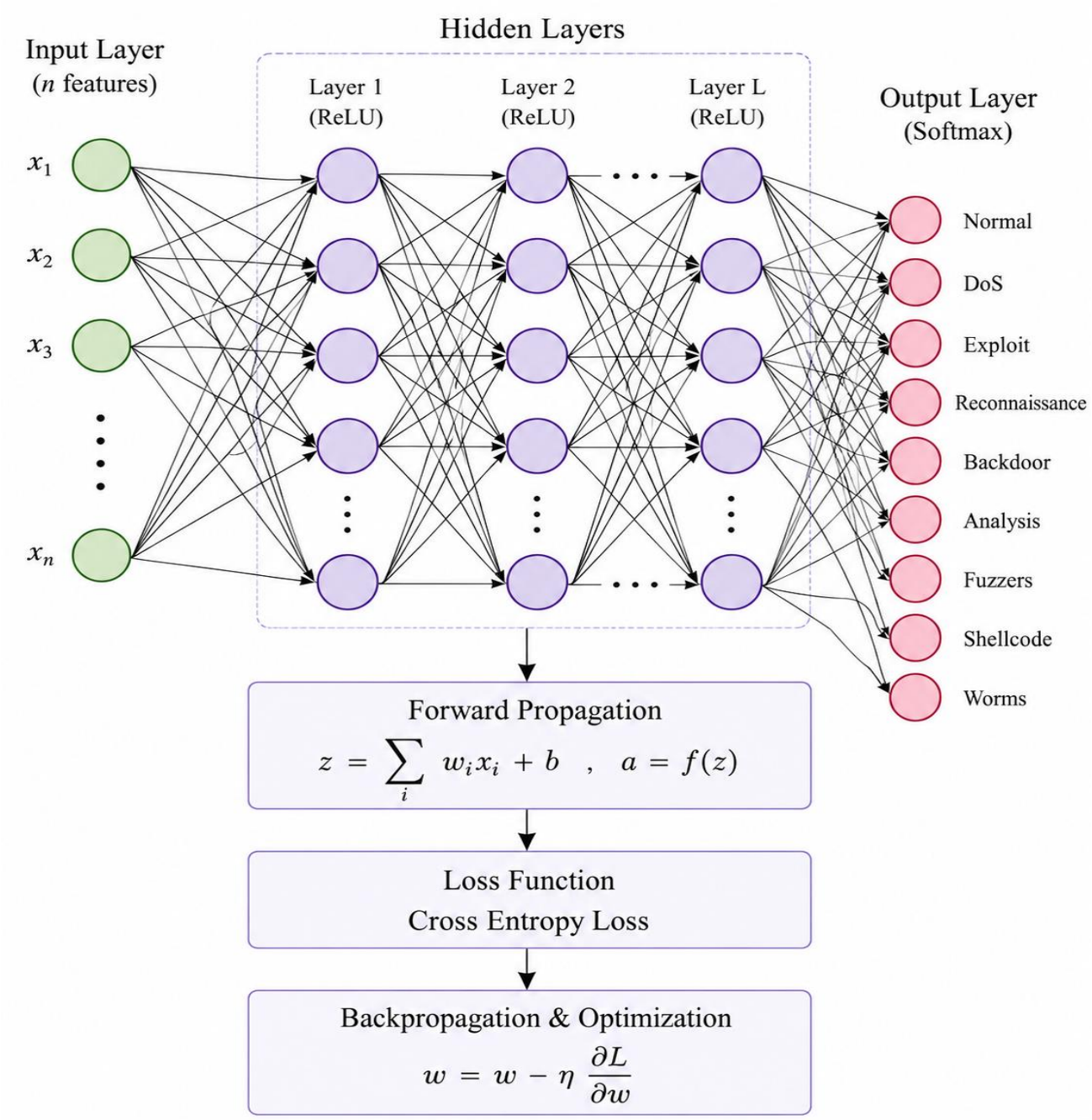


Fig. 5 DNN architecture

The output of a neuron is intended as:

$$z = \sum_{i=1}^{n} w_i x_i + b$$

where:

- w_i characterizes connection weights.
- x_i characterizes input features.
- b signifies bias.

The activated output is:

$$a = f(z)$$

where $f(z)$ is an activation function such as ReLU or Sigmoid.

The model parameters are enhanced using backpropagation:

$$w = w - \eta \frac{\partial L}{\partial w}$$

where:

- η is the learning rate.
- L is the loss function.

The DNN is used in this study for training complex attack signatures and hidden relationships in network traffic data. The model can automatically extract deep features from cybersecurity intelligence records, which can enhance the accuracy of attack classification and prediction.

3.4.4. Federated Learning (FL)

Federated Learning is the cornerstone of the Federated Sovereign AI Ecosystem, a crucial tool for intelligence sharing. Traditional machine learning approaches involve gathering data at a centralized location to train a model that is subsequently applied to every application, but in federated learning, the raw data are not sent between the various sovereign entities to train a global model [29].

Each sovereign node trains its own model using its own cybersecurity dataset and sends only the parameters of the model.

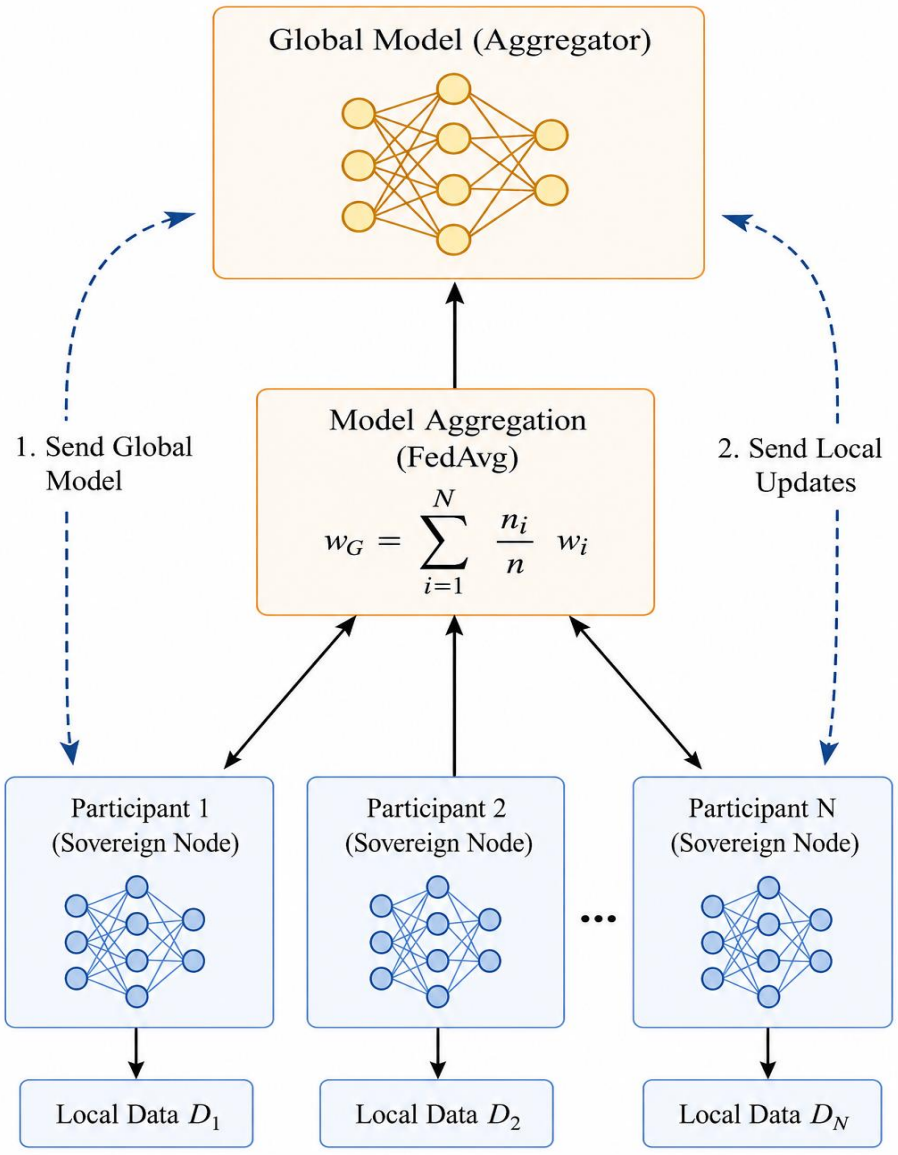


Fig. 6 FL architecture

The local model update is computed as:

$$w_i^{t+1} = w_i^t - \eta \nabla L_i(w_i)$$

where:

- w_i represents local model weights.
- η is the learning rate.
- L_i is the local loss function.

After local training, the federated coordinator aggregates model updates using the FedAvg algorithm:

$$w_G = \sum_{i=1}^{N} \frac{n_i}{n} w_i$$

where:

- w_G is the global model.
- n_i is the local data size.
- n is the total number of observations.

Then, the global model is redistributed to the sovereign nodes that took part in the training for further training iterations until convergence [30].

Federated learning advantages consist of data sovereignty, regulatory compliance, decreased privacy risks, and superior intelligent data creation abilities. Sovereigns can work together to advance the detection of cyber threats while their sensitive intelligence remains on the respective sovereign territories.

3.5. Performance Evaluation Metrics

Performance evaluation is an essential phase of the proposed Federated Sovereign AI Ecosystem because it measures the effectiveness of machine learning models, governance mechanisms, and cross-border intelligence interoperability.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1 = \frac{2PR}{P + R}$$

$$TrustIndex = \frac{\sum TS}{N}$$

$$IE = \frac{Successful\ Exchanges}{Total\ Exchanges}$$

$$CC = \frac{Data\ Shared}{Training\ Rounds}$$

4. Result and Analysis

The performance assessment of the proposed Federated Sovereign AI Ecosystem is provided in this section, based on the UNSW-NB15 and World Governance Indicators (WGI) datasets. The framework was evaluated with accuracy, precision, recall, F1-score, ROC-AUC, trust index, interoperability and cost of communication. The results of comparative analysis have proved the effectiveness of the proposed approach in the context of secure, trusted and privacy-preserving intelligence sharing across borders.

Overall, the results of the comparison clearly indicated that XGBoost performed best with an accuracy of 99.0%, precision of 99.5%, recall of 99.0%, and F1 score of 99.2% (as shown in figure 7). Random Forest also had consistent performance with an 98.1% accuracy, 98.6% precision, 98.4% recall, and 98.5% F1-score. The results for DNN were competitive with an accuracy of 97.2%, a precision of 97.8%, a recall of 97.8% and an F1-score of 97.8%. It is noteworthy, however, that Federated Learning had a lower performance, with an accuracy of 88.9%, precision of 86.9%, recall of 97.3% and F1-score of 91.8%, which reflects a higher sensitivity compared to the lower precision and overall classification performance.

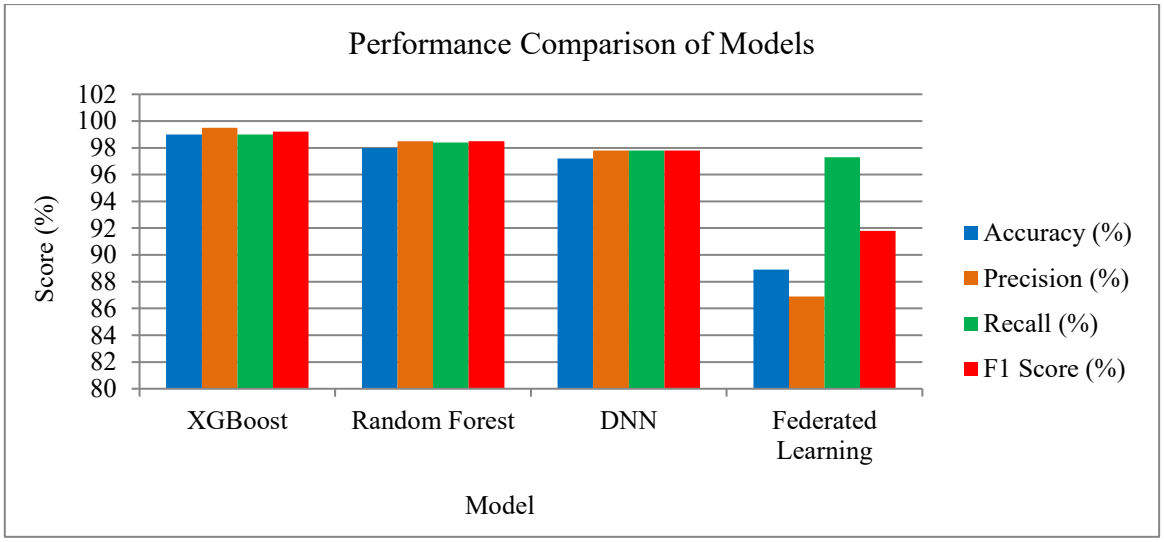


Fig. 7 Performance comparison of Learning models

Figure 8 shows that the proposed Federated Sovereign AI Ecosystem has consistently high trust and seamless interoperability among participating sovereign nodes. Denmark (95) was followed by Singapore (96), Switzerland (94.5), Finland (94) and Luxembourg (93.5). The relatively high threshold for trust is set at 70, with the medium threshold set at 40, and all values in the participating nodes are well above these levels, demonstrating that they meet the governance and security requirements for trusted collaboration. Moreover, the Intelligence Exchange Efficiency (IE%) achieved 100% for all 5 sovereign nodes, which means perfect exchange of information without any communication failures or loss of interoperability. The high uniformity of the performance of all participants further showcases the reliability and robustness of the proposed trust-aware federated approach to secure, reliable, and privacy-preserving cross-border intelligence sharing. Overall, the results support the framework's ability to enable trusted Governance and efficient interoperability, as well as reliable international cooperation on AI development, without loss of national data sovereignty.

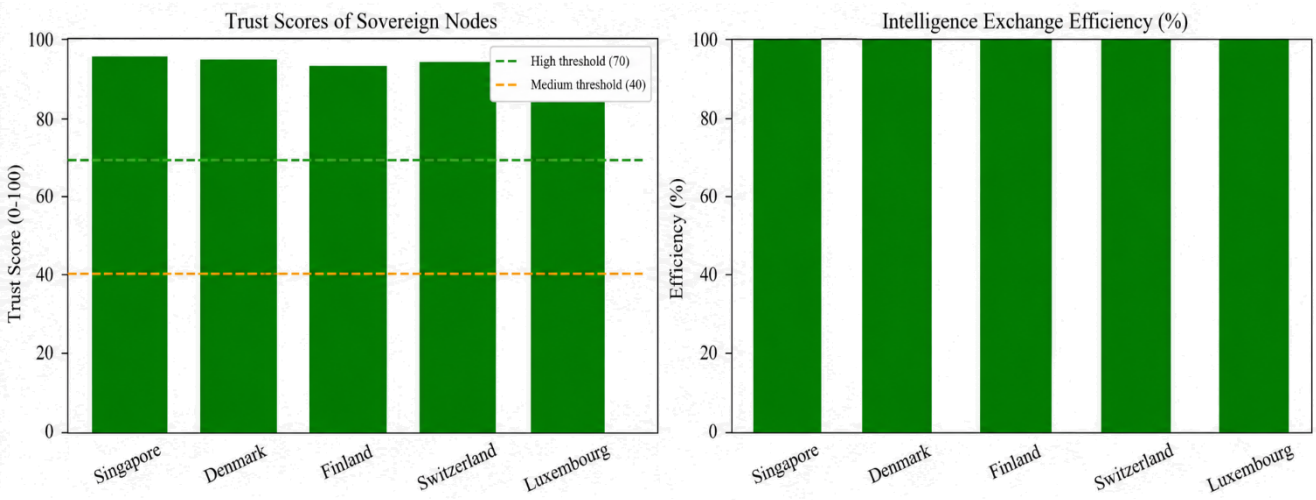
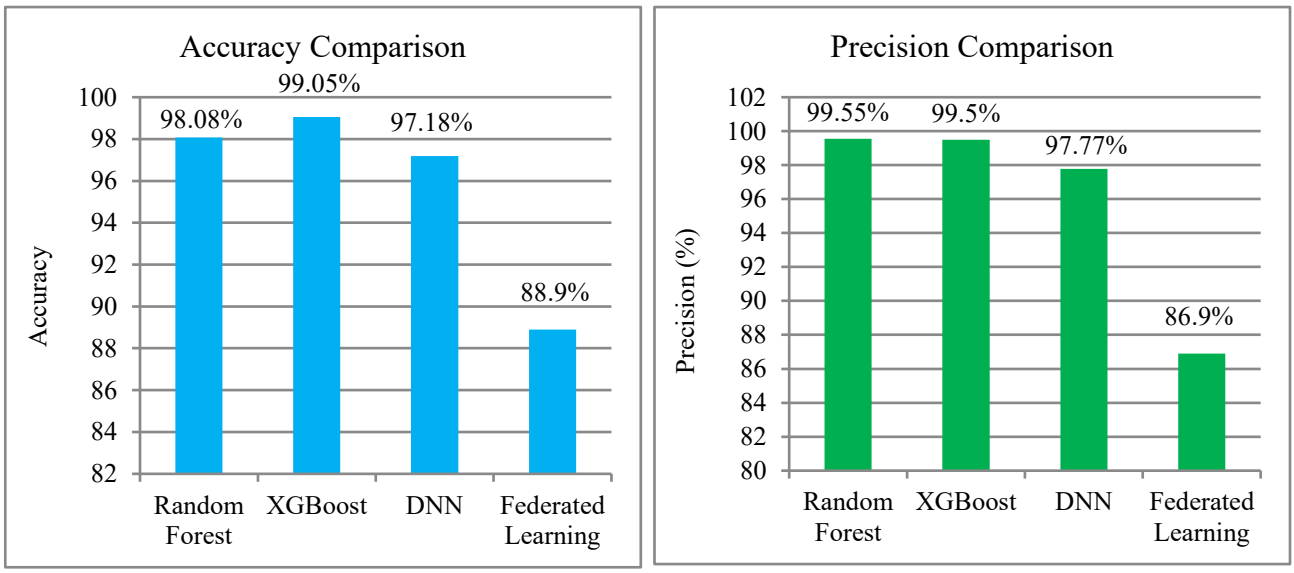


Fig. 8 Trust scores and intelligence exchange efficiency of sovereign nodes

From the results, as shown in Figure 9, it is clear that the XGBoost model was the most effective model with an overall accuracy of 99.05%, precision of 99.50%, recall of 99.01%, and an F1-score value of 99.25% in cyber threat detection. Random Forest was also competitive with 98.08% accuracy, 98.55% precision, 98.44% recall and 98.50% F1-score for classification, and DNN was also decent for the classification with 97.18% accuracy, 97.77% precision, 97.83% recall and 97.80% F1-score. The Federated Learning model achieved an accuracy of 88.90%, a precision of 86.90%, a recall of 97.31% and an F1-score of 91.81%. It was not as accurate or precise, but it had a good recall, thus good attack detection capabilities, while keeping data privacy. From the results, it is found that although the centralized learning approach ensures improved prediction, the federated learning approach is also suitable for prediction, privacy, security of collaboration and transborder intelligence sharing, with the two approaches being a good tradeoff.



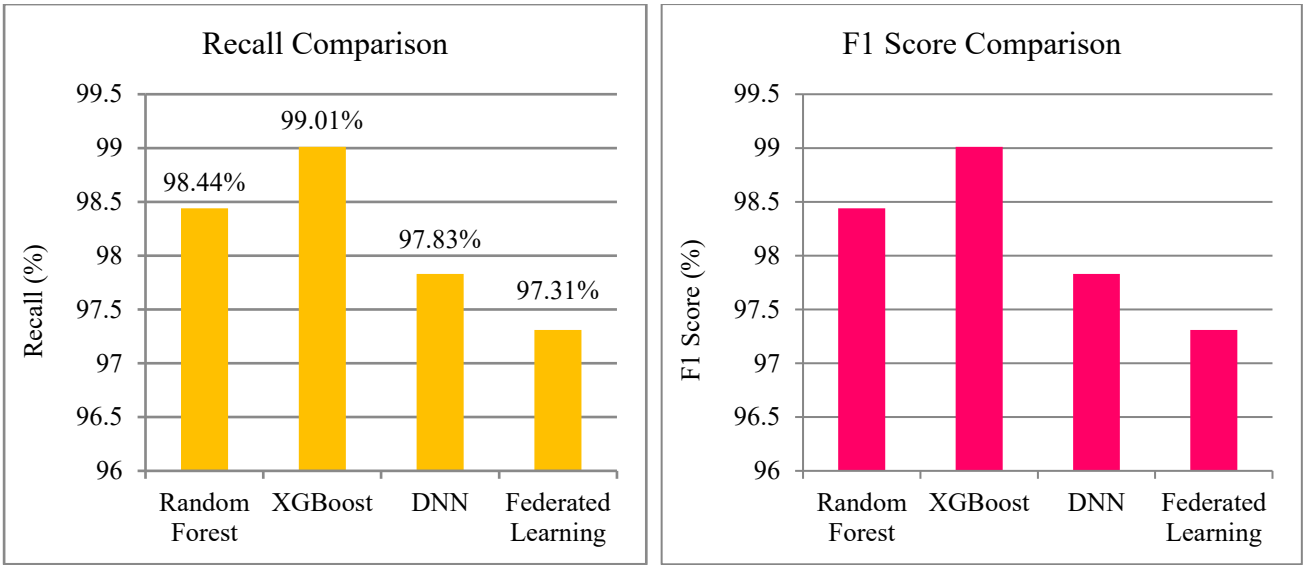


Fig. 9 Comparative performance of models using accuracy, precision, recall, and F1-score

As can be seen in Figure 10, results that are comprehensible are reached since it has developed a very high Trust Index (TI) of 94.56 and can therefore be assessed as highly reliable with a governance-compliant environment for sovereign participants to co-operate without restrictions. The overall exchange efficiency of Intel (IE%) was 100.00%. This is enabled through all intelligence information exchange without communication failures, packet loss and applicability failures. This result proves the importance of the trust-aware federated architecture for data sovereignty and easy cooperation. The amount of band width required to communicate the model parameter securely between the communicants during one communication round is reported as the communication cost in the framework, instead of the raw data to be communicated when it is being transmitted. Each round of communications costs 21,096.22 KB. There is an additional overhead involved in communicating in a federated manner, but it is manageable due to the level of security and privacy maintained and the governance compliance obtained. The high trust index, the perfect efficiency of the intelligence exchange and the manageable communication overheads show that the proposed Federated Sovereign AI Ecosystem offers a scalable, reliable and secure platform for trusted cross-border intelligence exchange and collaborative AI decision making.

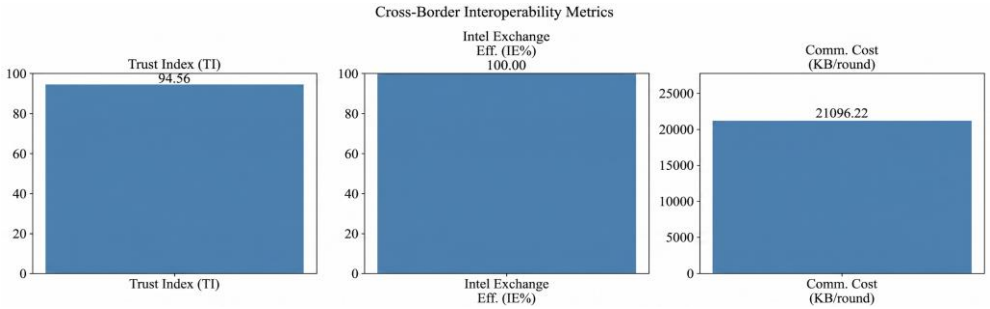


Fig. 10 Cross-border interoperability metrics

As can be seen in Figure 11, the model performs well in the first five rounds of communication. The accuracy stayed almost the same at 89.0% to 89.1%, and the precision showed some fluctuations at 87.2% to 87.5%. The highest values were for recall, consistently high, which implied a high detection capability throughout all training. The F1-score was around 90% for all rounds, indicating classification balance. All the evaluation criteria change slightly in each communication round, verifying the quick convergence of the entire criteria, smooth aggregation of the parameters, and steady learning in a collaborative way, revealing that the proposed federated learning framework can reliably show a stable relationship between the evaluation metrics and the communication rounds.

As observed in the figure 12, XGBoost achieved the highest performance with around 99.0 accuracy, 99.5 precision, 99.0 recall, and 99.3 F1, with consistently high results compared to the other models, namely Random Forest and DNN, which consistently outperformed 97% for all metrics. The best results were obtained using federated methods: FedAvg and Trust-Weighted FL, with nearly 88.9% accuracy, 86.9% precision, 97.3% recall, and 91.8% F1-score, respectively, while Multi-Round FL slightly increased to 89.1% accuracy, 87.4% precision, 96.9% recall, and 91.9% F1-score. Overall, the results show that centralized models hold significant advantages over federated learning approaches, with “multi-round federated learning” showing slight improvement over traditional FL.

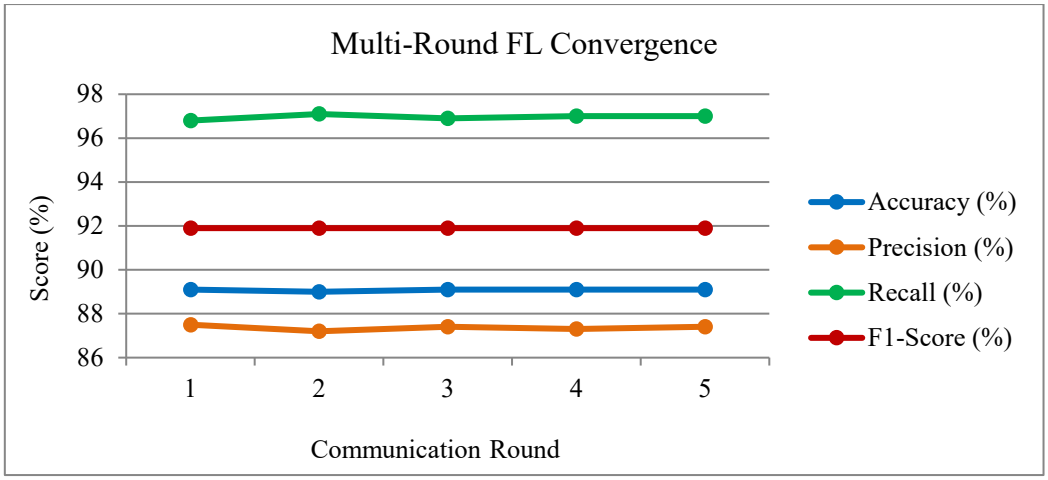


Fig. 11 Multi-round federated learning convergence across communication rounds

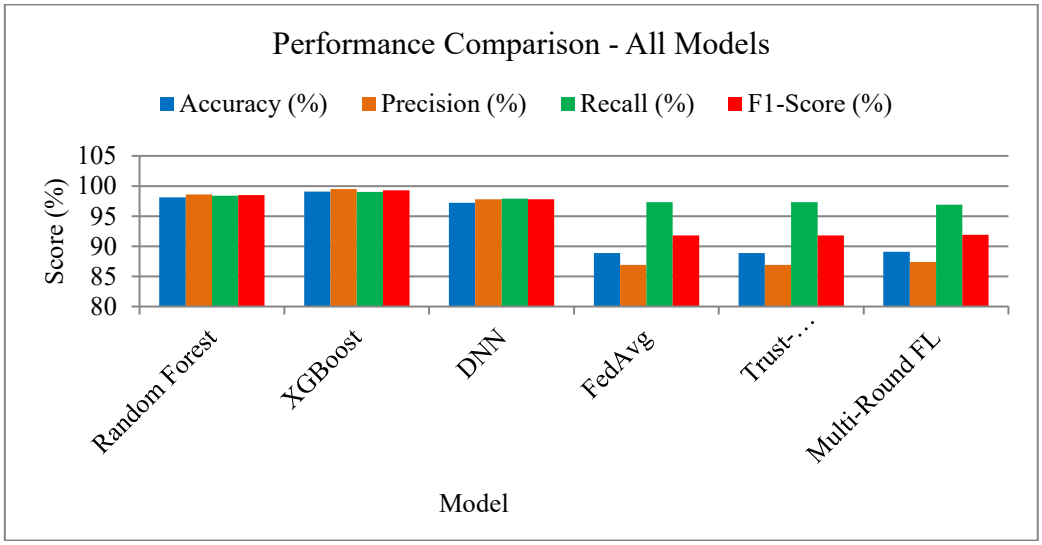


Fig. 12 Performance comparison of centralized and federated learning models

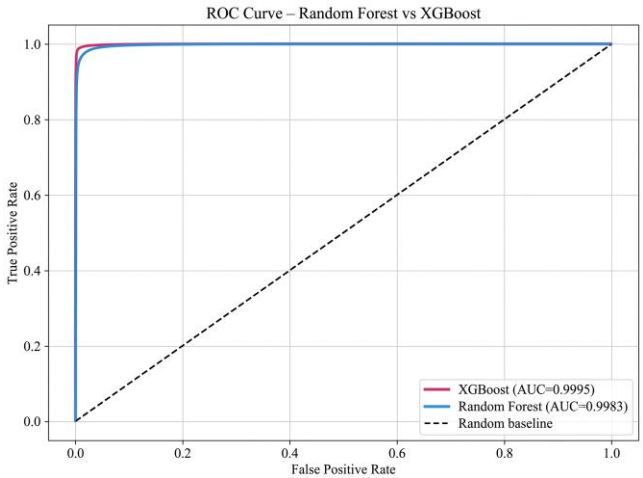


Fig. 13 ROC curve comparison of Random Forest and XGBoost classifiers

The two models seem to have good classification results, as shown in Figure 13. The Area under the Curve (AUC) was used as the criterion to assess the classifiers, and XGBoost gave the best result of 0.9995, followed by Random Forest with 0.9983. Both ROC curves are very close to the upper left corner, signifying that the true positive rates are high and false positive rates are low for a range of decision thresholds. Both classifiers perform significantly better than a random baseline (AUC of 0.50), thus demonstrating excellent discriminative performance. Altogether, Random Forest is slightly better than XGBoost and is the best choice to make accurate and reliable predictions.

From the figure 14, it is evident that XGBoost performed best with 18,436 True Negatives, 32,609 True positives, 164 False positives, and 326 False negatives as compared to the others. The number of correctly classified normal and attack samples is 18124 and 32421, respectively, while 476 samples are classified as false positive and 514 samples are classified as false negatives by the Random Forest. DNN has achieved an accuracy of 87.16%, correctly identifies 17,864 normal samples and identifies 32,219 attack samples, while 736 and 716 samples have been classified as false positive and false negatives, respectively. Overall, XGBoost has the best detection ability; Random Forest has an advantage over DNN in the classification accuracy reduction and reliability of prediction.

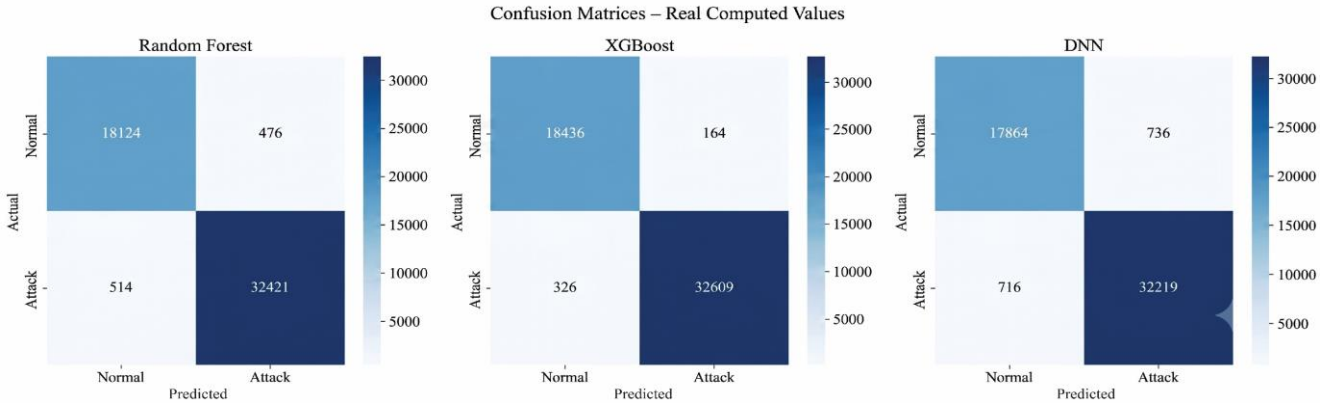


Fig. 14 Confusion matrix comparison of Random Forest, XGBoost, and DNN classifiers

As seen in figure 15, Xavier's Decision Forests (XGBoost) gives the highest overall accuracy (99.1%), precision (99.5%), recall (99.0%) and F1 score (99.3%). Followed by Random Forest and DNN. With the removal of the centralized learning, performance dropped to 88.9% accuracy, 86.9% precision, 97.3% recall, and 91.8% F1-score when using FedAvg. For the Multi-Round FL and Trust-Weighted FL, similar performance was observed except for an insignificant drop in recall (96.9%), which led to a modest improvement in accuracy (89.1%), precision (87.4%) and F1-score (91.9%). These results validate the advantages of iterative federated optimization as compared to traditional federated learning.

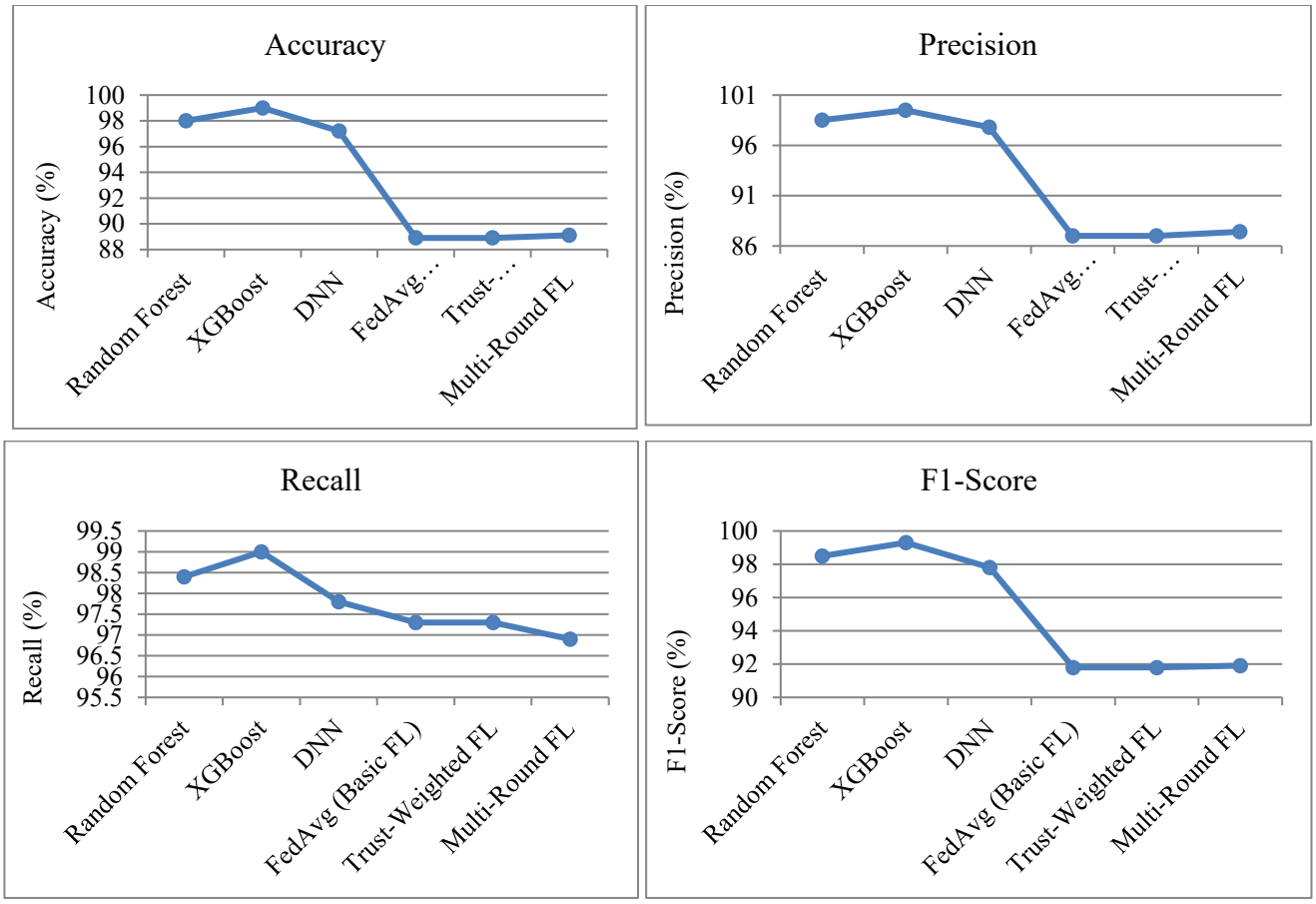


Fig. 15 Ablation study comparing centralized and federated learning models

5. Conclusion

This proposed Federated Sovereign AI Ecosystem (FSAIE) clearly illustrates how it is possible to share intelligence data securely across borders, maintaining data sovereignty and meeting governance compliance requirements. Experimental results on UNSW-NB15 and World Governance Indicators (WGI) datasets demonstrated that XGBoost provides the best predictive performance with 99.05% accuracy, 99.50% precision, 99.01% recall and 99.25% F1-score compared to Random Forest (98.08% accuracy) and DNN (97.18% accuracy). The Federated framework proposed a good detection accuracy of 89.10%, a precision of 87.40%, a recall of 96.90%, and an F1 Score of 91.90% while ensuring data privacy. Trust evaluation yielded a Trust Index of 94.56, while the scores of sovereign nodes lie in the range of 93.5-96.0, and its Intelligence Exchange Efficiency is 100%, which ensures seamless interoperability between participating countries. The overhead of communication stayed moderate with 21,096.22KB per round, and the multi-round federated learning showed that the model converged and maintained a high accuracy (89.0-89.1%) through 5 communication rounds. Moreover, XGBoost also demonstrated the best AUC of 0.9995, and it only had 164 false positives and 326 false negatives, demonstrating its best threat detection. In general, the framework is a scalable, trustworthy, and governance-centric approach to collaborative international AI and cyber intelligence sharing.

References

[1] Swarna Bindu Chetty et al., "Sovereign AI for 6G: Towards the Future of AI-Native Networks," *arXiv preprint*, pp. 1-8, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Adebayo Nurudeen Kalejaiye, "Federated Learning in Cybersecurity: Privacy-Preserving Collaborative Models for Threat Intelligence Across Geopolitically Sensitive Organizational Boundaries," *International Journal of Advance Research Publication and Review*, vol. 2, no. 7, pp. 227-250, 2025. [CrossRef] [Google Scholar]

[3] Taiwo Justice Olorunlana, "Securing the Global Cloud: Addressing Data Sovereignty, Cross-Border Compliance, and Emerging Threats in a Decentralized World," *International Journal of Science, Architecture, Technology, and Environment*, vol. 2, no. 5, pp. 1394-1407, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Venkata Satya Sai Ajay Daliparthi et al., "Digital Sovereignty for Collaborative AI Engineering: A Survey," *IEEE Access*, vol. 13, pp. 216438-216465, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] Waseem Nasir, and P. Kumar, "Integrating Policy, Technology, and Intelligence in Federated Cybersecurity Frameworks," 2025. [Google Scholar]

[6] Yu Chen, "AI Sovereignty: Navigating the Future of International AI Governance," pp. 1-28, 2024. [Google Scholar] [Publisher Link]

[7] Chaudhary Hamza Riaz, and Muhammad Usman Hadi, "Cross-Border Intelligence: Defending AI Innovation in the Age of Digital Sovereignty and GDPR," *SSRN*, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[8] Obehi Irekponor, "Designing Resilient AI Architectures for Predictive Energy Finance Systems Amid Data Sovereignty, Adversarial Threats, and Policy Volatility," *International Journal Advance of Research Publication and Reviews*, vol. 2, no. 6, pp. 73-100, 2025. [CrossRef] [Google Scholar]

[9] Mayowa Emmanuel, "AI-Driven Energy Finance Systems Aligned with Cross-Border Data Sovereignty Laws," 2025. [Google Scholar]

[10] Laxman Singh et al., "Adaptive Hybrid Intelligence Framework for Proactive Cross-Border Fraud Detection in Electronic Transaction Ecosystems," *Journal of Scientific Innovation and Advanced Research*, vol. 1, no. 7, pp. 1-10, 2025. [Google Scholar] [Publisher Link]

[11] Yik Chan Chin et al., "Interoperability in AI Safety Governance: Ethics, Regulations, and Standards," *arXiv preprint*, pp. 1-122, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[12] Md Tarek Hasan, and Sai Praveen Kudapa, "Data Privacy-Aware Machine Learning and Federated Learning: A Framework for Data Security," *American Journal of Interdisciplinary Studies*, vol. 2, no. 3, pp. 1-34, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Clara Maathuis, and Kasper Cools, "Digital Sovereignty Control Framework for Military AI-based Cyber Security," *arXiv preprint*, pp. 1-10, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Boyang Dong, and Zhengyi Zhang, "AI-Driven Framework for Compliance Risk Assessment in Cross-Border Payments: Multi-Jurisdictional Challenges and Response Strategies," *Spectrum of Research*, vol. 4, no. 2, pp. 1-24, 2024. [Google Scholar] [Publisher Link]

[15] Prem Pradeep Motgi, "Federated Infrastructure Blueprints for Sovereign AI: Cross Border Workload Orchestration and Data Localization," *International Journal of Engineering Technology Research and Management*, vol. 10, no. 6, pp. 97-109, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[16] Segun Odion, and Santosh Reddy Addula, "AI Risk Governance for Advancing Digital Sovereignty in Data-Driven Systems: An Integrated Multi-Layer Framework," *Future Internet*, vol. 18, no. 4, pp. 1-30, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[17] Shalabh Kumar Singh, and Shubhashis Sengupta, "Sovereign AI: Rethinking Autonomy in the Age of Global Interdependence," *arXiv preprint*, pp. 1-11, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Avinash Agarwal, and Manisha J. Nene, "A Federated Architecture for Sector-Led AI Governance: Lessons from India," *Transforming Government: People, Process and Policy*, pp. 1-14, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[19] Sreenivasulu Gajula, "Federated Intelligence in Financial Ecosystems: A Privacy-Preserving AI Framework for Cross-border Risk Analysis," *Journal of Information Systems Engineering and Management*, vol. 10, no. 60s, pp. 1040-1048, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Daniel Foster, "Machine Learning-Based Privacy Preservation and Data Governance in Cross-Border Data Sharing," 2026. [Google Scholar]

[21] Alejandro López et al., "Adaptive Collaborative Intelligence Models for Real-Time Threat Analysis under Cross-Border Cyber Incidents and Governmental Emergency Protocols,". [Google Scholar]

[22] Jiling Lin, "Design and Simulation of a Federated Learning-based Multilateral Data Privacy Protection and Ethical Collaborative Governance Model for Cross-Border E-Commerce," *Proceedings of the 2025 5th International Conference on Internet of Things and Machine Learning*, Association for Computing Machinery, New York, NY, United States, pp. 324-330, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[23] Meena P. Subramanian, "The Influence of Federated AI on Data Sovereignty in Global Enterprises," *International Journal of Scientific Research and Engineering Trends*, vol. 10, no. 4, pp. pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Kaggle, UNSW-NB15, Kaggle. [Online]. Available: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15

[25] World Bank Group, Worldwide Governance Indicators, World Bank Group, 2025. [Online]. Available: https://www.worldbank.org/en/publication/worldwide-governance-indicators

[26] Fortune Ifeanyi, and Victor Eze, "IoT Threat Detection using Federated Learning and Edge AI with Random Forest Optimization," *Nature Journal of Emerging Sciences Technologies and Innovations*, vol. 3, no. 2, pp. 92-103, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jiaqi Zhao et al., "SXGB: Secure and Efficient Vertical Federated XGBoost via Trusted Execution Environments," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 2, pp. 2275-2288, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[28] Marco Röder, Peter Kowalczyk, and Frédéric Thiesse, "Leveraging the Potentials of Federated AI Ecosystems," *Innovation Through Information Systems: Volume III: A Collection of Latest Research on Management Issues*, vol. 48, pp. 61-68, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] Tymoteusz Miller et al., "Federated Learning for Environmental Monitoring: A Review of Applications, Challenges, and Future Directions," *Applied Sciences*, vol. 15, no. 23, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] Adil Akhmetov, Batyr Sharimbayev, and Mohammed Alaa Ala'anzy, "Personalized Federated Learning for Sovereign Personal AI Agents: A Review," *2026 18th International Conference on Electronics, Computer, and Computation (ICECCO)*, Kaskelen, Kazakhstan, pp. 1-6, 2026. [CrossRef] [Google Scholar] [Publisher Link]