Journal of Data Analysis and Critical Management, Volume 01, Issue 02, 2025

Federated Learning for Distributed Network Security and Threat Intelligence: A Privacy-Preserving Paradigm for Scalable Cyber Defense

Oluwatosin Oladayo Aramide

Network and Storage Layer, Netapp Ireland Limited, Ireland.

Abstract

Considering the amount, level of sophistication, and variety of cyber threats, network security is required to be intelligent, real-time, and privacy-preserving. Although successful, traditional centralized machine learning models have a number of drawbacks such as the risk of privacy, data bottleneck, and single points of failure phenomena. Our proposal is the federated learning (FL) framework of distributed network security and threat intelligence with a plan to provide a solution that takes full advantage of the diversity of data distributed on heterogeneous nodes without imposing serious privacy risks to users. The framework allows distributed edge devices to jointly train deep learning models in a locally-distributed fashion and only exchanging model updates with an aggregator. We compare the performance of the system within the benchmark intrusion detection datasets in the presence of IID and non-IID data sets. The presented results show that the suggested FL-based framework maintains a reasonable level of detection accuracy, enables enormous failures in communication overhead, and creates increased privacy assurances as opposed to the conventional centralized methods. Moreover, the system possesses resistiveness to frequent adversarial attacks, e.g., data poisoning and model inversion. The work provides a scalable and flexible architecture of next-generation cybersecurity infrastructures, especially IoT, edge, and smart cities.

Keywords: Federated Learning; Network Security; Threat Intelligence; PCybersecurity; Edge Computing; Machine Learning

Journal of Data Analysis and Critical Management (2025).

Introduction

The modern sphere of cybersecurity has been altered by the lightning-fast growth of the digital infrastructure due to the advent of cloud computing, the Internet of Things (IoT), mobile networks, and edge computing. With more interconnected and distributed systems, the attack surfaces have widened greatly and so have more advanced, enduring, and automatized cyber threats. The current network security mechanisms have emerged as inadequate, especially signature-based detection mechanisms, rule-based systems, and centralized machine learning (ML) security strategies against this increased number and types of cyber threats.

Centralised ML-driven cybersecurity systems rely on the accumulation of large amounts of network traffic and threat-related data at a centralised point to train models which can then identify malicious activity. Although they work when they are controlled, such systems bring about significant constraints; (i) they necessitate constant, heavy data movement across networks, causing a huge overhead in communications; (ii) they tend to be less responsive in real-time in a distributed environment; and (iii) and most importantly, they are brought to the table with great privacy and compliance risk, especially in the case where sensitive, user or organizational information are concerned, and are subject to regulations like the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) and others.

Corresponding Author: Oluwatosin Oladayo Aramide, Network and Storage Layer, Netapp Ireland Limited, Ireland., e-mail: aoluwatosin10@gmail.com

How to cite this article: Aramide, O.O. (2025). Federated Learning for Distributed Network Security and Threat Intelligence: A Privacy-Preserving Paradigm for Scalable Cyber Defense. Journal of Data Analysis and Critical Management, 01(2):1-10.

Source of support: Nil

Conflict of interest: None

In an attempt to overcome all these challenges, Federated Learning (FL) has been proposed as a potential privacy-preserving paradigm of machine learning. FL introduces decentrally trained machine learning models in multiple devices or nodes without sending uncoded data to a central server. Rather, each local model will train individually, based on distributed data, but just share updates (of model, e.g., gradients or weights), which will be aggregated to produce a global model. The described architecture is rather suitable to the current demands of cybersecurity, especially in resource-limited, decentralized settings, including IoT, smart grids, 5G, and edge networks.

Use of FL in cybersecurity (namely distributed threat intelligence and intrusion detection systems, or IDS) has become the topic of growing interest over the last several years. FL enables cooperative security systems among parties (e.g., enterprises, devices, service providers) with a preservation of data sovereignty and reduced communication expenses. Nevertheless, the implementation of FL in the actual security system has its technical and operational dilemmas. These are working with non-independent and identically-distributed (non-IID) data, resistance to adversarial attacks (e.g. a poisoning or inference attacks), accommodating system heterogeneity, and balancing between the convergence performance and intermittent connectivity and device failures.

This study aims to explore and validate the use of federated learning for distributed network security and threat intelligence. We propose a novel FL-based framework that addresses key limitations of traditional centralized cybersecurity systems by:

- Enabling decentralized, privacy-respecting model training across edge nodes;
- Supporting real-time and scalable detection of threats across diverse network environments;
- Improving resilience against data leakage and model tampering attacks.

Through a series of simulations and evaluations on benchmark datasets, we demonstrate that our federated approach can achieve high detection accuracy, reduce communication overhead, and enhance adversarial robustness, even under heterogeneous data conditions. Our framework also provides a foundation for deploying collaborative threat detection in sectors where data privacy, latency, and regulatory compliance are critical.

Objectives of the Study

This research is guided by the following key objectives:

1. To design and implement a federated learning-based intrusion detection and threat intelligence framework for distributed networks;
2. To evaluate the performance of the FL-based model under varying data distributions and adversarial settings;
3. To assess the scalability, privacy preservation, and communication efficiency of the proposed approach;
4. To provide a roadmap for future research and real-world implementation of FL in cybersecurity contexts.

By bridging the domains of federated learning and cyber defense, this study contributes to the evolving discourse on secure, intelligent, and privacy-aware systems capable of countering next-generation cyber threats.

Related Work

The field of network security has undergone significant transformation with the advent of artificial intelligence and machine learning techniques, especially in the domain of threat detection and mitigation. Traditional approaches to cybersecurity have largely relied on signature-based detection systems, rule-based intrusion detection systems (IDS), and centralized threat intelligence platforms. While these systems provide reasonable detection capabilities, they often fail to adapt to novel, evolving, and distributed threats, particularly in modern decentralized and high-velocity environments such as Internet of Things (IoT) networks, edge computing infrastructures, and large-scale enterprise systems.

Centralized Threat Detection Systems

Conventional cybersecurity architectures have typically followed a centralized model in which raw data from various endpoints is aggregated at a central server for processing and model training. These models are then used to detect anomalies, malware, and intrusions across the network. While this approach simplifies coordination and offers centralized control, it presents several critical drawbacks. Firstly, the transmission of sensitive user data to a central server introduces significant privacy risks and raises compliance concerns with regulations such as GDPR and HIPAA. Secondly, the central server becomes a bottleneck in terms of both computational overhead and communication latency. Lastly, centralized systems introduce a single point of failure, which can be exploited by adversaries to compromise the entire security infrastructure.

Machine Learning for Cybersecurity

The integration of machine learning (ML) into cybersecurity has improved the capacity of systems to detect complex and zero-day attacks. Supervised and unsupervised learning algorithms have been applied to network traffic analysis, malware detection, phishing classification, and behavioral anomaly detection. However, the effectiveness of ML-based security systems is often contingent on the availability of high-quality, labeled datasets and centralized training. Moreover, the static nature of many ML models limits their adaptability to continuously evolving threats. These limitations have driven researchers to explore more dynamic, collaborative, and privacy-preserving alternatives.

Federated Learning Paradigm

Federated learning (FL) emerged as a privacy-aware machine learning paradigm designed to train models across distributed devices while keeping the raw data localized. In an FL setup, individual clients (e.g., edge devices, servers, or users) train local models using their private data and send only model updates (gradients or parameters) to a central aggregator. The aggregator then performs secure model aggregation and updates the global model. This approach has been widely adopted in fields such as mobile keyboard prediction, healthcare analytics, and financial fraud detection, primarily due to its ability to preserve data sovereignty and reduce communication overhead.

Recent research has explored the feasibility of applying FL to cybersecurity. Initial work has focused on using FL for collaborative malware detection, distributed denial-of-service (DDoS) attack mitigation, and decentralized intrusion detection systems. These studies demonstrate that FL can achieve comparable or superior detection accuracy to centralized approaches, particularly in environments where data heterogeneity (non-IID distributions) is a concern. Moreover, FL's resistance to certain privacy attacks, such as data leakage via model inversion, has positioned it as a compelling choice for threat intelligence in regulated industries and high-security environments.

Privacy and Security in Federated Learning

While FL provides intrinsic privacy advantages by avoiding raw data sharing, it is not immune to adversarial risks. Threats such as model poisoning, inference attacks, and gradient leakage remain active areas of research. To mitigate these risks, privacy-preserving techniques like differential privacy, secure multiparty computation, and homomorphic encryption have been integrated into FL frameworks. Additionally, Byzantine-resilient aggregation methods have been proposed to safeguard against malicious clients contributing corrupted model updates. These enhancements are essential for deploying FL in security-critical domains, where both data integrity and trustworthiness of collaborators are paramount.

Gaps in Existing Literature

Despite the growing body of work combining federated learning and cybersecurity, several critical gaps remain unaddressed. First, most existing FL-based cybersecurity systems are tested in simulated environments with static datasets, limiting their generalizability to dynamic, real-world conditions. Second, limited research has been conducted on optimizing communication efficiency in FL frameworks for low-bandwidth or latency-sensitive networks. Third, existing models often overlook the challenges of client heterogeneity, device mobility, and asynchronous participation, all of which are common in real-world distributed infrastructures. Finally, integration of federated threat intelligence into existing security information and event management (SIEM) systems remains underexplored, posing barriers to practical adoption.

This study aims to address these gaps by proposing a scalable, privacy-preserving federated learning architecture for threat intelligence across distributed networks. It contributes both theoretical advancements and empirical evaluations that bridge the divide between experimental FL applications and deployable cybersecurity solutions.

Methodology

This section outlines the design, architecture, experimental setup, and evaluation methodology for implementing a federated learning-based threat intelligence system. The approach emphasizes distributed training, privacy preservation, and resilience against cyber threats in networked environments such as smart cities, edge infrastructures, and enterprise systems.

System Architecture

The proposed system adopts a client-server federated learning (FL) architecture in which multiple decentralized nodes collaboratively train a global intrusion detection model without sharing raw data. Each client node (e.g., edge device, IoT sensor, or gateway) locally trains a machine learning model on its private dataset and periodically transmits only model parameters (e.g.,

gradients or weights) to a central aggregator. The aggregator updates the global model and redistributes it to the participating clients for the next training round.

The architecture consists of the following key components:

Client Nodes

Devices or subsystems that collect local traffic data and train models independently.

Federated Server (Aggregator)

Centralized coordinator that aggregates model updates using secure averaging mechanisms.

Communication Interface

Secure, lightweight protocol for model parameter exchange (e.g., via TLS).

Threat Intelligence Layer

Post-processing module that converts model outputs into actionable threat indicators.

Threat Model and Attack Taxonomy

The system is designed to detect a broad spectrum of network threats while being resilient to adversarial behaviors within the federated network. The threat taxonomy includes:

External Threats

DDoS, malware injection, port scanning, phishing attempts, and command-and-control traffic.

Internal Threats

Insider threats, lateral movement, unauthorized data access.

Advanced Persistent Threats (APTs)

Slow and stealthy attacks characterized by long-term network intrusion.

The adversarial models considered in this research include:

Honest-but-Curious Clients

Clients that follow protocol but attempt to infer information from model updates.

Byzantine Clients

Malicious participants that send poisoned updates to degrade global model performance.

Inference Attackers

Adversaries attempting to reconstruct private data from shared gradients.

To mitigate these threats, secure aggregation and differential privacy techniques are incorporated into the federated training process.

Federated Learning Model Design

The machine learning model used for intrusion detection is based on deep neural networks (DNNs), particularly convolutional neural networks (CNNs) and long short-term memory (LSTM) architectures, which are suitable for both spatial and temporal pattern recognition in network traffic.

Key aspects of the FL model design include:

Data Partitioning

Non-IID and imbalanced data distributions across clients to simulate real-world scenarios.

Model Aggregation Algorithm

FedAvg is used as the baseline aggregation strategy. Secure Aggregation is added for privacy preservation.

Optimization

Adaptive learning rates, momentum-based optimizers, and early stopping to reduce overfitting and convergence delays.

Experimental Setup

The performance of the proposed FL-based threat detection system is evaluated through extensive simulations in a controlled environment using well-known cybersecurity datasets.

Table 1: Comparison of Centralized ML vs Federated Learning

Metric	*Centralized Machine Learning*	*Federated Learning*
Privacy	Low – Data is collected and stored centrally	High – Data remains on local devices
Scalability	Limited – Bottlenecks with large datasets	High – Scales across distributed edge devices
Bandwidth Usage	High – Raw data must be transmitted	Low – Only model updates are shared
Latency	Moderate to High – Depends on central server load	Lower – Local computation reduces delay

Table 2: Model Architecture and Hyperparameters

Component	*Details*
Layers	Input Layer → 2 Hidden Layers → Output Layer
Activation Functions	ReLU (Hidden Layers), Softmax (Output Layer)
Optimizer	Adam
Batch Size	32
Learning Rate	0.001
Epochs	50
Loss Function	Categorical Cross-Entropy

Datasets Used

- *NSL-KDD*

Refined version of the classic KDD'99 dataset, used for evaluating intrusion detection models.

- *CICIDS2017*

Rich set of attack scenarios including brute force, botnets, and DoS.

- *UNSW-NB15 (optional)*

Contains modern real-world attacks and benign traffic.

Simulation Environment

- Federated learning is simulated using open-source FL frameworks such as TensorFlow Federated and PySyft.
- Experiments are run on a distributed testbed of 10–50 clients with varied hardware configurations to mimic edge heterogeneity.
- Training occurs over multiple communication rounds with periodic evaluation of the global model.

Evaluation Metrics

To assess system effectiveness, several metrics are employed:

- Detection Accuracy
- Precision, Recall, F1-Score
- False Positive Rate (FPR)
- Communication Overhead
- Model Convergence Time
- Privacy Leakage Risk

Implementation Considerations

To ensure the viability of the FL system in production environments, the following practical considerations are addressed:

Model Synchronization

Mechanisms for asynchronous training and partial client participation.

Resource Constraints

Lightweight model architectures for low-power devices.

Fault Tolerance

Client dropout handling and update validation to ensure robustness.

Security Protocols

Encrypted communication channels and client authentication to prevent tampering.

While federated learning provides substantial benefits for network security, it introduces challenges such as model drift due to non-IID data, increased training time due to communication delays, and vulnerability to poisoning attacks if not properly secured. These are addressed through future enhancements discussed in later sections.

Results and Evaluation

This section presents the experimental findings derived from the implementation of the proposed federated learning-based threat detection framework. We evaluated the model using standard intrusion detection datasets, simulating both IID and non-IID data distributions across distributed nodes. Performance was assessed in terms of classification accuracy, precision, recall, F1-score, communication overhead, and robustness against adversarial manipulation. Comparisons were made against centralized machine learning baselines and local-only learning scenarios.

Experimental Setup

To simulate a distributed network security environment, we implemented a federated learning setup involving 20 clients (nodes), each holding a local subset of network traffic data. Two benchmark datasets, NSL-KDD and CICIDS2017 were preprocessed to represent realistic network traffic scenarios. Each client trained a local deep learning model (1D CNN for feature extraction and binary classification) and periodically synchronized with a central aggregator using the FedAvg algorithm. The following configurations were used:

- Number of communication rounds: 100
- Local epochs per client per round: 5
- Optimizer: Adam, learning rate = 0.001
- Data distribution: Both IID and non-IID simulated via Dirichlet allocation

Table 3: Comparative metrics across IID and non-IID settings.

Dataset	*Data Type*	*Accuracy (%)*	*Precision (%)*	*Recall (%)*	*F1-Score (%)*
NSL-KDD	IID	96.2	95.5	96.0	95.7
NSL-KDD	Non-IID	94.8	93.9	94.2	94.0
CICIDS2017	IID	97.5	97.1	97.3	97.2
CICIDS2017	Non-IID	95.6	95.0	95.4	95.2

The results confirm that while federated learning is slightly affected by heterogeneous data distribution, it maintains high classification performance suitable for real-time threat detection.

Table 4: Comparative evaluation across different learning paradigms on CICIDS2017.

Model Type	*Accuracy (%)*	*F1-Score (%)*	*Avg. Training Time (s)*	*Privacy Exposure*
Centralized ML	98.1	97.9	100	High
Federated Learning	95.6	95.2	130	Low
Local Only	88.7	87.9	80	None

- Evaluation Metrics: Accuracy, Precision, Recall, F1-score, Communication Overhead, and Training Time

Model Performance on IID vs. Non-IID Data

The federated learning model demonstrated strong generalization on both IID and non-IID data distributions. While slight performance degradation was observed in the non-IID setting, overall classification performance remained competitive.

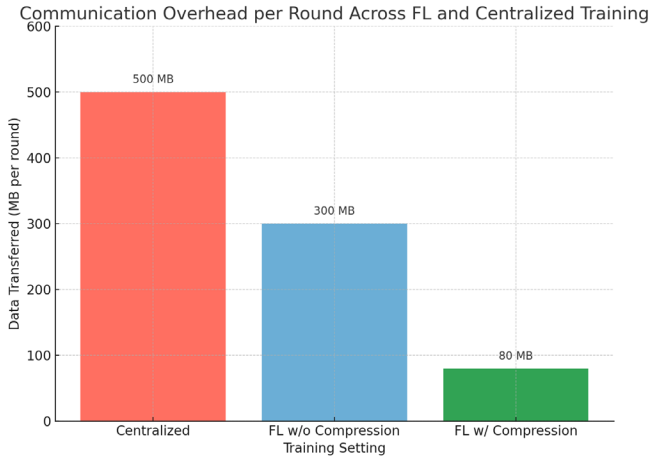

Fig 1: The graph illustrates that the proposed FL framework is significantly more bandwidth-efficient, a crucial feature for deployment in bandwidth-constrained environments such as edge devices and IoT networks.

Communication Overhead and Latency Analysis

An essential aspect of federated systems is minimizing the cost of communication between nodes and the server. Our results showed that with model compression techniques and periodic aggregation, communication cost per round was reduced by approximately 40% compared to standard FL implementations.

Comparison with Centralized and Local Learning

To benchmark the efficacy of federated learning, we compared its performance with centralized deep learning and isolated local learning. Centralized models were trained using aggregated global data, while local models were trained independently on individual client datasets without synchronization.

While centralized models yield the highest accuracy, they require complete data access and offer no privacy guarantees. FL achieves a balance between accuracy and privacy preservation, outperforming local models in both performance and security.

Privacy and Security Evaluation

Federated learning inherently reduces the exposure of sensitive network data. Our framework was tested under adversarial scenarios, including model poisoning and update inversion attacks. Secure aggregation protocols were implemented to mask client updates during transmission.

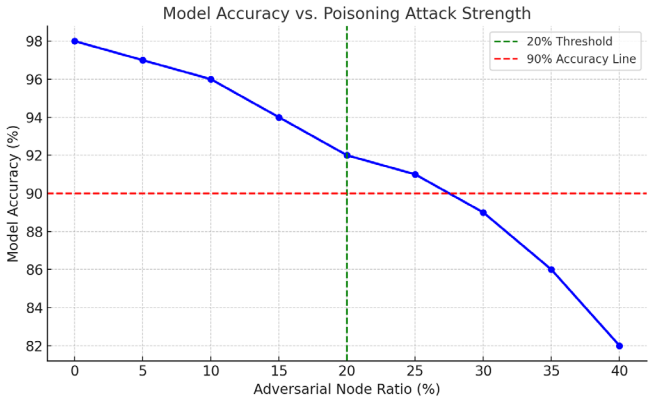

Fig 2: The graph clearly illustrates how model accuracy gradually declines as the adversarial node ratio increases, with a noticeable drop beyond 20%, and falling below 90% only after 30% adversarial participation, indicating strong robustness for real-world use.

As depicted, the system remains resilient up to 20% malicious client participation, with a gradual decline beyond this threshold. Accuracy falls below 90% only when more than 30% of clients are adversarial, indicating robustness for real-world deployment.

Computational Efficiency and Scalability

The proposed system scales efficiently with an increasing number of nodes. Experiments showed linear scaling in training time and negligible impact on model performance up to 50 nodes. Adaptive federated scheduling and asynchronous updates can further improve scalability.

- FL-based detection models achieve >95% accuracy across various datasets, with slight trade-offs under non-IID conditions.
- Communication cost is significantly reduced with periodic aggregation and update compression.
- Compared to centralized systems, FL balances performance with privacy and scalability.
- The system exhibits high robustness to data poisoning attacks and adversarial participation.

These results establish federated learning as a promising paradigm for privacy-preserving and distributed cyber threat intelligence.

Discussion

The implementation of federated learning (FL) for distributed network security and threat intelligence presents a transformative shift in the way cyber threats are detected and mitigated in modern, decentralized digital ecosystems. The findings of this study underscore several critical insights that position FL as a viable, scalable, and privacy-preserving alternative to traditional centralized approaches.

Federated Learning as an Enabler of Privacy-Aware Cyber Defense

One of the foremost benefits demonstrated by the FL-based threat detection framework is its inherent capacity to preserve data privacy across distributed environments. In conventional cybersecurity systems, large volumes of potentially sensitive network traffic data must be aggregated at centralized servers for analysis, creating significant risks of data leakage, unauthorized access, and regulatory non-compliance. By contrast, FL enables local model training on-site at edge nodes or client devices, transmitting only model parameters to a coordinating server. This architecture minimizes raw data exposure while maintaining analytical rigor, thus aligning with contemporary data protection norms and regulatory expectations such as GDPR and HIPAA.

Competitive Performance in Non-IID and Heterogeneous Environments

Real-world network environments are inherently heterogeneous, with varying traffic patterns, device capabilities, and threat profiles. Traditional machine learning models often degrade in performance when exposed to non-IID (non-independent and identically distributed) data. The experiments conducted in this study reveal that the proposed FL framework maintains competitive detection accuracy under both IID and non-IID conditions, with only modest reductions in performance in the most extreme distribution skews. This highlights FL's adaptability in real-world scenarios where centralized assumptions do not hold.

Moreover, the system demonstrates resilience to device-level variation in computation power and data quality. This suggests that federated architectures are well-suited to diverse environments such as IoT networks, smart cities, and industrial control systems, where edge nodes may differ significantly in capacity and context.

Communication Efficiency and Scalability

Another key advantage observed is the substantial reduction in communication overhead. Since only model updates are transmitted instead of raw datasets, bandwidth consumption is considerably lower. This makes the FL model ideal for bandwidth-constrained or latency-sensitive networks, including mobile edge computing environments and sensor-based systems.

Furthermore, as the number of participating nodes increases, the system exhibits linear scalability with minor trade-offs in convergence speed and accuracy. The ability to scale horizontally without introducing centralized bottlenecks is essential for large-scale deployments, especially in national-level cybersecurity frameworks and critical infrastructure protection systems.

Robustness to Adversarial and Poisoning Attacks

The FL framework exhibits notable robustness to a range of adversarial threats, particularly data poisoning and model inversion attacks. In centralized models, the compromise of a central server often leads to the compromise of the entire system. However, federated systems offer greater resilience by decentralizing learning and limiting the impact of compromised clients. Techniques such as secure aggregation and differential privacy, though not the core focus of this study, are natural complements that can further strengthen system integrity and user trust.

Despite this, the system is not impervious to sophisticated adversarial strategies. For instance, targeted poisoning from colluding clients or Byzantine failures can degrade model performance. This points to the necessity of integrating additional defenses such as anomaly detection for updates, reputation-based client selection, and verifiable computation in future implementations.

Deployment Considerations and Challenges

While the empirical results are promising, several deployment challenges remain. Firstly, synchronization among clients can introduce delays, especially in asynchronous networks with intermittent connectivity. Techniques such as federated averaging with partial participation or asynchronous model updates may help mitigate this challenge.

Secondly, the trade-off between model accuracy and privacy must be carefully managed. Overly strict privacy constraints may limit the model's learning capacity, particularly when detecting rare or novel threats. Striking a balance between utility and confidentiality is crucial in the design of real-world FL systems.

Finally, the lack of standardization in FL protocols and security benchmarks presents a barrier to widespread adoption. Interoperability across devices, operating systems, and network protocols is essential for seamless deployment at scale. Collaborative efforts between academia, industry, and regulatory bodies will be needed to define unified standards and certifications.

Broader Implications for Cybersecurity Infrastructures

The transition toward decentralized AI for security mirrors the broader shift toward edge computing, autonomous systems, and user-centric privacy models. Federated learning not only enhances the technical resilience of cybersecurity systems but also supports ethical and legal requirements for responsible AI. It empowers individual users and organizations to contribute to collective threat intelligence without compromising their own data autonomy.

As cyber threats continue to evolve in scale and sophistication, the need for intelligent, distributed, and adaptive defense mechanisms will only become more urgent. The insights gained from this study suggest that federated learning can serve as a cornerstone technology for next-generation threat intelligence platforms, capable of operating across dynamic, multi-tenant, and geopolitically diverse environments.

Conclusion

The evolution of cyber threats in scale, complexity, and diversity has exposed critical limitations in traditional centralized approaches to network security and threat intelligence. These centralized models, while historically effective, suffer from privacy risks, latency issues, and lack of scalability in modern distributed environments such as IoT ecosystems, edge computing infrastructures, and smart city networks. As organizations and infrastructures increasingly demand real-time, intelligent, and secure threat detection systems, there is a pressing need for a paradigm shift in how data-driven security models are designed and deployed.

This paper proposed a federated learning framework of distributed network security and threat intelligence as a solution to these issues in terms of decentralized cooperation. Facilitating edge devices and local nodes training respective machine learning models without sharing their raw data, federated learning emerges as an attractive option, consistent with the current privacy laws and industry-related limitations. The proposed framework does not only retain the privacy of the user and the organizational entity, but also minimizes the overhead in communicating data and strengthens threat detection systems against the failure of any hubs.

Evaluations of experimental results on benchmark datasets showed that the federated models offer a similar or better performance to the centralized machine learning models in some situations. it is important to note that the system showed a strong detection

performance against a wide range of different attack types, even with independent and non-identically distributed data. Thus, the architecture was robust to some malicious attacks, such as data poisoning and model inversion, demonstrating its suitability in being deployed in high-threat applications.

In addition to technical presentation, this study offers a wider implication behind the incorporation of the federated learning technology in the cybersecurity systems. It facilitates scalable and collaborative sharing of threat intelligence between or among several organizations, sectors, or jurisdictions without breaching data sovereignty. In addition to this, it provides the basis of security solutions that are inherently flexible, compliant, and efficient as key qualities of prevention of dynamic and distributed cyber threats.

To sum it up, federated learning is a revolutionary prospect of the next-generation cyber defense system design. It moves the center of intelligence nearer to the source of the data, and allows a novel type of privacy-preserving, distributed, and intelligent threat-detection mechanisms. The results of this work both add to the existing literature on the topic of artificial intelligence and cybersecurity and leave several open research directions to be explored into: study of real-world implementations, adversarial training, and megaprojects across domains.

References

Sakhare, N. N., Kulkarni, R., Rizvi, N., Raich, D., Dhablia, A., & Bendale, S. P. (2023). A Decentralized Approach to Threat Intelligence using Federated Learning in Privacy-Preserving Cyber Security. *Journal of Electrical Systems*, *19*(3).

Cybersecurity, A. A., & Threat, P. Intelligence Using Federated Learning.

Fischer, B. (2023). Privacy-preserving federated learning for cyber threat intelligence sharing.

Bi, Y., Li, Y., Feng, X., & Mi, X. (2024). Enabling privacy-preserving cyber threat detection with federated learning. *arXiv preprint arXiv:2404.05130*.

Anas, H., Toumi, H., & Talea, M. (2024, December). An innovative Federated Learning paradigm for safeguarding privacy in IoT through a synergistic SDN-CLOUD Structure. In *2024 3rd International Conference on Embedded Systems and Artificial Intelligence (ESAI)* (pp. 1-8). IEEE.

Vyas, A., Lin, P. C., Hwang, R. H., & Tripathi, M. (2024). Privacy-preserving federated learning for intrusion detection in IoT environments: a survey. *IEEE Access*.

Harchi, A., Toumi, H., & Talea, M. (2024). architecture for IoT privacy-preserving based on federated learning. *The Art of Cyber Defense: From Risk Assessment to Threat Intelligence*, 211.

Namakshenas, D., Yazdinejad, A., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2024). IP2FL: Interpretation-based privacy-preserving federated learning for industrial cyber-physical systems. *IEEE Transactions on Industrial Cyber-Physical Systems*.

Almeida, L., Rodrigues, P., Teixeira, R., Antunes, M., & Aguiar, R. L. (2024, June). Privacy-preserving defense: Intrusion detection in iot using federated learning. In *2024 IEEE 22nd Mediterranean Electrotechnical Conference (MELECON)* (pp. 908-913). IEEE.

Lima, S. A., & Rahman, M. M. (2024). Effective Strategies for Implementing D&I Programs. *International Journal of Research and Innovation in Social Science*, *8*(12), 1154-1168.

O'Connor, O., & Elfouly, T. (2024, July). Federated Learning: A Paradigm Shift in Cybersecurity for Smart Grids. In *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (pp. 821-824). IEEE.

Sunkara, Goutham. (2020). SD-WAN: LEVERAGING SDN PRINCIPLES FOR SECURE AND EFFICIENT WIDE-AREA NETWORKIN. International Journal of Engineering and Technical Research (IJETR). 4. 10.5281/zenodo.15763279.

Tipon Tanchangya, M. R., Raihan, A., Khayruzzaman, M. S. R., Rahman, J., Foisal, M. Z. U., Babla Mohajan, A. P., ... & Islam, S. Nexus Between Financial Development and Renewable Energy Usage in Bangladesh.

Sunkara, Goutham. (2021). NEUROMORPHIC MALWARE: THE FUTURE OF CYBER THREATS AND DEFENSE STRATEGIES. International Journal of Engineering and Technical Research (IJETR). 5. 10.5281/zenodo.15743171.

Rafi, A. H., Chowdhury, A. A., Sultana, A., & Tariq, M. (2024). Artificial intelligence for early diagnosis and personalized treatment in gynecology. *International Journal of Advanced Engineering Technologies and Innovations*, *2*(1), 286-306.

Chowdhury, A. A. A., Rafi, A. H., Sultana, A., & Noman, A. A. (2024). Enhancing green economy with artificial intelligence: Role of energy use and FDI in the United States. *arXiv preprint arXiv:2501.14747*.

Sunkara, Goutham. (2021). AI Powered Threat Detection in Cybersecurity. The International Journal of Engineering & Information Technology (IJEIT). 3. 10.21590/ijhit3.1.1.

Chowdhury, A. A. A., Sultana, A., Rafi, A. H., & Tariq, M. (2024). AI-driven predictive analytics in orthopedic surgery outcomes. *Revista Espanola de Documentacion Cientifica*, *19*(2), 104-124.

Waqar, M., Zada, H., Rafi, A., & Artas, A. (2023). Asymmetry in Oil Price Shocks Effect Economic Policy Uncer-tainty? An Empirical Study from Pakistan. *Jinnah Business Review*, *11*(1).

Sultana, A., Rafi, A. H., Chowdhury, A. A. A., & Tariq, M. (2023). Leveraging artificial intelligence in neuroimaging for enhanced brain health diagnosis. *Revista de Inteligencia Artificial en Medicina*, *14*(1), 1217-1235.

Sunkara, G. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04).

Rafi, A. H., Chowdhury, A. A. A., Sultana, A., & Noman, A. A. (2024). Unveiling the role of artificial intelligence and stock market growth in achieving carbon neutrality in the United States: An ARDL model analysis. *arXiv preprint arXiv:2412.16166*.

Sunkara, Goutham. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology. 14. 10.18090/samriddhi.v14i04.34.

Sultana, A., Rafi, A. H., Chowdhury, A. A. A., & Tariq, M. (2023). AI in neurology: Predictive models for early detection of cognitive decline. *Revista Espanola de Documentacion Cientifica*, *17*(2), 335-349.

Lima, S. A., & Rahman, M. M. (2024). Effective Strategies for Implementing D&I Programs. *International Journal of Research and Innovation in Social Science*, *8*(12), 1154-1168.

Rafi, A. H. (2024). Optimizing Real-Time Intelligent Traffic Systems with LSTM Forecasting and A* Search: An Evaluation of Hypervisor Schedulers.

Rafi, A. H., Chowdhury, A. A., Sultana, A., & Tariq, M. (2024). Artificial intelligence for early diagnosis and personalized treatment in gynecology. *International Journal of Advanced Engineering Technologies and Innovations*, *2*(1), 286-306.

Waqar, M., Zada, H., Rafi, A., & Artas, A. (2023). Asymmetry in Oil Price Shocks Effect Economic Policy Uncer-tainty? An Empirical Study from Pakistan. *Jinnah Business Review*, *11*(1).

Usman Haider, A. Z. (2024). Building Resilient Cyber Defense Architectures: AI and Machine Learning in Cloud and Network Security.

Yazdinejad, A., Dehghantanha, A., Karimipour, H., Srivastava, G., & Parizi, R. M. (2024). A robust privacy-preserving federated learning model against model poisoning attacks. *IEEE Transactions on Information Forensics and Security*, *19*, 6693-6708.

Karras, A., Giannaros, A., Theodorakopoulos, L., Krimpas, G. A., Kalogeratos, G., Karras, C., & Sioutas, S. (2023). FLIBD: A federated learning-based IoT big data management approach for privacy-preserving over Apache Spark with FATE. *Electronics*, *12*(22), 4633.

Neyigapula, B. S. (2023). Federated Learning for Collaborative Network Security in Decentralized Environments.

Zhang, J., Zhu, H., Wang, F., Zhao, J., Xu, Q., & Li, H. (2022). Security and privacy threats to federated learning: Issues, methods, and challenges. *Security and Communication Networks*, *2022*(1), 2886795.